UNIVERSIDAD CARLOS III DE MADRID

Grado en Ingeniería Informática

Mención en Ingeniería de Computadores

TRABAJO FIN DE GRADO

Adaptación del Cliente del Servicio de Sellado Espacio-Temporal de CERTILOC a un Dispositivo Móvil

AUTOR: Sergio Blanco Domínguez

TUTOR: Ana Isabel González-Tablas Ferreres

Septiembre de 2013

AGRADECIMIENTOS

Querido lector,

Espero me disculpe por el lenguaje utilizado en los siguientes párrafos. Le prometo que el resto del documento tendrá un lenguaje más formal.

Por extraño que parezca, a mí no me ha resultado especialmente difícil redactar este apartado. A lo mejor porque tengo claro a quien le debo haber llegado tan lejos. O quizá tenga algo que se me permita el libre albedrío a la hora de escribir. Sea como fuera, heme aquí, redactando los agradecimientos de todo un Trabajo Fin de Grado. Y eso me hace recordar el comienzo de todo este ciclo de la vida llamado "universidad", hace ya cuatro años.

Podría decirse que soy uno de los últimos estudiantes que desean sacar buenas calificaciones solo por su orgullo personal (y no por necesidad, para seguir estudiando) pero eso no quita que el viaje haya sido uno de los más emocionantes de mi vida. Quizá estas sean palabras más para un recién entrado en la universidad que para alguien que lea un TFG, pero la universidad no es solo el aprendizaje de diversas materias, sino también para el *mundo exterior*, esa bestia que espera a que salgas para acabar contigo. Sin embargo, no es tan difícil enfrentarse a ella. Y sin duda alguna la universidad te pone a prueba con "prácticas" constantes para que puedas mirar a esa bestia a los ojos.

"*¿Por qué nos caemos? Para aprender a levantarnos*"[1]

Dicho esto, y ya que quedan más de cien páginas para que pase el rato leyendo cosas más interesantes que mis pensamientos, pasemos directamente a los agradecimientos.

Como no, el primer agradecimiento debe ser para mis padres, José y Trinidad. Primero, por querer tenerme. Segundo, por haberme criado de la forma que lo han hecho, pues no sería lo que soy ni pensaría como pienso de no ser por ellos. Y tercero, por aguantarme en mis malos momentos, que no son pocos. Debería seguir este texto

[1] Michael Caine – Batman Begins.

mencionando a mis tíos, por sus diversos consejos, y a mis abuelos, por venderme tan bien por el barrio. Pero son tantos nombres que no acabaríamos nunca, así que solo os diré "*GRACIAS*" a todos vosotros.

Siguiendo los agradecimientos no puede faltar un nombre aquí: Alex. Compañero no solo de prácticas, sino también de muchas comidas y cenas e incluso viajes al norte. Solo lamento no haberte conocido antes, haber coincidido desde el instituto o el colegio, pues mi vida habría sido de otra manera hasta llegar aquí. Sin embargo, he de decirte que a veces "*tu carencia de fe resulta molesta*"[2], sobre todo en época de exámenes o entregas. No obstante, espero seguir viéndote (y quedándonos hasta las tantas de la madrugada matando perros de tres cabezas) durante mucho tiempo.

Aunque no solo Alex me ha soportado como compañero de prácticas. Algunos otros me han sufrido y he tenido que sufrirles en estos cuatro años (mas lo segundo que lo primero). Sin embargo, de todo ese grupo quiero mencionar especialmente a dos personas, Marta y Paty. Porque no tengo la menor duda de que sin su ayuda, yo no estaría aquí hoy y tendría que esperar un año más para poder llamarme ingeniero. En momentos puntuales fueron dos personas que estuvieron ahí para ayudarme y eso es digno de elogiar. Y de agradecer.

Por supuesto, tengo que agradecerle a Anabel muchas cosas, pero dos en particular. La primera, haberme aceptado como su alumno en este proyecto y haber confiado en mí para continuar *su legado* al mundo de la seguridad, el proyecto CERTILOC. La segunda, haber aguantado un intenso verano lleno de dudas, correos y peticiones por mi parte sin haberme mandado a cocinar un rato, que estaba en su derecho.

También quiero mencionar a mis amigos, esos que ya estaban antes de comenzar este viaje y aún continúan a mi lado. En especial a Elia y Ale, que aun estudiando y acabando sus propias carreras, han estado a mi lado para apoyarme cuando fue necesario.

---

[2] James Earl Jones – Star Wars: Episodio IV - Una Nueva Esperanza.

Y por fin, el que para mí es el agradecimiento más especial. El agradecimiento a una persona que me ha apoyado, ayudado y animado más que nadie. Alguien a quien he soportado y aguantado menos de lo que ella ha tenido que aguantarme y soportarme a mí. Alguien que empezó como compañera de prácticas, para acabar siendo mi compañera en la vida. Gracias por todo, Jessica. "*El mundo es más interesante contigo dentro*"[3].

Podría tirarme más rato aquí escribiendo nombres de compañeros o amigos que han estado conmigo en estos cuatro años, pero se nos acaba el tiempo y las hojas para los agradecimientos. Así que solo mencionaré algunos de sus nombres: Leonor, Javi, Ángel, Jesús… A todos vosotros, gracias.

Sin más demora, querido lector, le dejo con la culminación de la que ha sido mi obra durante estos cuatro años en la universidad.

A más ver.

Madrid, Septiembre de 2013.

[3] Anthony Hopkins – El Silencio de los Corderos.

RESUMEN

El presente documento describe el procedimiento seguido para la realización del Trabajo Fin de Grado, desarrollado por el alumno Sergio Blanco Domínguez, para la obtención del título de Grado en Ingeniería Informática.

El proyecto se engloba dentro del proyecto de investigación CERTILOC, uno de cuyos objetivos es proporcionar Servicios de SELLADO Espacio-Temporal (SSET) mediante Sellos Espacio-Temporales (SET). Los SET son documentos digitales que acreditan que un sujeto generó una firma digital sobre un documento en una supuesta zona, determinada por un punto espacial de origen y un intervalo de tiempo.

En el Proyecto Fin de Carrera "Análisis, diseño e implementación de mejoras en el servicio de sellado espacio-temporal de CERTILOC", de Raúl David Martínez Calmaestra, se implementó un sistema para la generación de sellos espacio-temporales. Es dicho sistema, el sujeto utilizaba un cliente Java estándar desde el que se conectaba a dos módulos (CERTILOC y TSA) que proporcionaban la información espacio-temporal del sujeto mediante documentos confiables, a partir de los cuales se construía el SET.

El objetivo de este TFG es la adaptación del módulo cliente desarrollado en el PFC mencionado a un dispositivo móvil. Ésta será la primera aproximación al despliegue de un servicio de este tipo en dispositivos móviles, en este caso a un dispositivo con sistema operativo Android, y deberá de poder ejecutar el módulo cliente desde el dispositivo y comunicarse con CERTILOC y TSA para generar el SET. La solución finalmente desarrollada utiliza, además de las entidades ya incorporadas al sistema, un servicio de firma digital (Digital Signature Service). Aparte de ofrecer las mismas funcionalidades que el sistema del que se parte, el cliente desarrollado en este TFG aporta una interfaz gráfica para la generación, validación y visualización de los detalles del SET más acorde con un dispositivo móvil.

ABSTRACT

This document describes the procedure followed to implement the Final Project, developed by Sergio Blanco Domínguez, to obtain the title of Computer Engineering.

This project is part of the research project CERTILOC; one of its objectives is to provide Spatial-Temporal Stamping Services (STSS) by Spatial Temporal Stamps (STS). STS are digital documents that prove that a subject generated a digital signature on a document in a supposed area, determined by a spatial origin point and time interval.

In the Degree Project "Análisis, diseño e implementación de mejoras en el servicio de sellado espacio-temporal de CERTILOC", by Raúl David Martínez Calmaestra, it's implemented a system to generate spatial-temporal stamps. In that system, a subject used a Java standard client which connected to two modules (CERTILOC and TSA) that provides the spatial-temporal information of the subject by trusted documents, with which generate the STS. The purpose of this project is the adaptation of the client module developed in the aforementioned Degree Project to a mobile device. This will be the first approximation to deployment this service on mobile devices, in this case to an Android device, and should be executed the client module from the device and communicate with CERTILOC and TSA to generate STS. The solution developed uses, besides entities already incorporated into the system, a Digital Signature Service (DSS). Besides offering the same functionality as the previous system, the client developed in this project provides a graphical interface for the generation, validation and visualization of STS details optimized for a mobile device.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

El presente documento describe el Trabajo Fin de Grado (TFG) realizado por el autor para la obtención del título de Grado en Ingeniería Informática.

Este proyecto consiste en la adaptación del cliente del servicio de sellado espacio-temporal implementado en "Análisis, diseño e implementación de mejoras en el servicio de sellado espacio-temporal de CERTILOC" [1], de Raúl David Martínez Calmaestra, a un dispositivo móvil con sistema operativo Android.

En este capítulo se presentará el contexto del proyecto CERTILOC y del trabajo [1], introduciendo los conceptos esenciales de los mismos; y se detallarán los principales objetivos que persigue este TFG. Finalmente, se expondrá la estructura de contenidos del presente documento.

1.1. Contexto: El Proyecto CERTILOC

CERTILOC es el nombre de un proyecto de investigación financiado por el Ministerio de Educación y Cultura, que ha llevado a cabo por el Grupo de Seguridad en las Tecnologías de la Información y las Comunicaciones de la Escuela Politécnica Superior de la Universidad Carlos III de Madrid.

Parte de dicho proyecto se refleja en la Tesis Doctoral [3] de la tutora del presente TFG, Dña. Ana Isabel González-Tablas Ferreres, donde se expone el modelo teórico de una arquitectura informática que permita certificar la localización espacio-temporal de un dispositivo o la acción sobre un documento, sin afectar a la privacidad de la información que contiene. Por lo tanto, es preciso introducir y explicar los conceptos mencionados.

Se puede definir la **información espacio-temporal** como la ubicación de un elemento en un determinado momento. Dicha información es utilizada a diario en prácticamente cualquier ámbito; desde el registro de entrada a una fábrica mediante tarjeta electrónica, hasta en algo tan simple como pasar lista en una clase de primaria.

La forma de representar esta información ha variado con el paso del tiempo y la evolución de las tecnologías, pero desde el uso de "*tercera calle a la derecha, a 15 minutos andando*" ya se daba información espacio-temporal de un elemento. Actualmente se utilizan tecnologías de ubicación geográfica por satélite (GPS) para indicar localizaciones espaciales y el tiempo universal coordinado (UTC) para indicar situaciones temporales.

De la misma forma que hay diferentes métodos para representar la información, existen diferentes maneras de obtener la información. Se pueden distinguir dos principales formas de obtenerla: un **sistema de localización** determina la información espacio-temporal de un elemento; o el **propio elemento** obtiene su propia información espacio-temporal. Sin embargo, sea cual sea la forma de obtener la información, no se garantiza que la información sea la correcta y no haya sido alterada.

Es por ello que CERTILOC introduce el término de **certificado espacio-temporal** (CET), un documento electrónico que asocia un sujeto a una determinada información espacio-temporal, garantizando que dicha información no ha sido alterada. Para poder construir un CET es necesario contar con un sistema de localización que garantice su autenticidad. El certificado es emitido por una entidad de confianza, por lo que permite que un tercero confíe en esta información.

Para realizar un CET en CERTILOC, se construye un documento XML digital que contiene, al menos, un identificador del sujeto, una localización espacial, un instante temporal y una firma digital sobre todo lo anterior generada por la entidad de confianza. El servicio que genera los CET se denomina en CERTILOC **Servicio de Acreditación Espacio-Temporal (SAET)**.

Adicionalmente, cuando la información espacio-temporal está asociada a una persona física, se entra en el ámbito de la **privacidad de datos personales**, determinado por la Ley 15/99, Orgánica de protección de datos de carácter personal, 1999. Dicha Ley establece que el afectado debe poder decidir para qué y cómo se procesan dichos datos.

Para resolver esta cuestión, como se menciona en [4], *en CERTILOC se incorpora un mecanismo para gestionar y proteger la privacidad, basado en el establecimiento de políticas de privacidad asociadas a cada dispositivo localizable. Dichas políticas indican cuándo y dónde puede ser localizado el dispositivo, así como quién tiene derecho a hacerlo y de qué forma.*

Hasta la fecha, cuatro han sido los Proyectos Fin de Carrera previos que han trabajado en implementar las funcionalidades de CERTILOC mencionadas hasta ahora (consúltese [4], [5], [6] y [7]).

Adicionalmente, CERTILOC especifica también los denominados **Servicios de Sellado Espacio Temporal** (**SSET**) a través de los **sellos espacio-temporal** (**SET**). Los SET son documentos digitales que establecen dónde y cuándo cierta entidad Sujeto S realiza determinada acción sobre un documento digital M. En el caso particular del proyecto CERTILOC, lo que se sella (o acredita) es el momento y lugar de la generación de una firma digital sobre el documento.

Para generar un SET en CERTILOC (véase la Ilustración 1), un Sujeto S solicita un CET y, tras recibirlo, genera una firma digital sobre el CET y el documento M que desea firmar. Posteriormente, solicita un **sello temporal** (**ST**) sobre la firma resultante, que es un documento digital que establece que un documento existía antes de determinado momento. Los sellos temporales los emite una autoridad de confianza denominada Autoridad de Sellado Temporal o por las siglas TSA (derivadas del término en inglés *Time Stamping Authority*). Para terminar de realizar el SET, se concatena el documento M, el CET, la firma sobre M y CET y el ST.

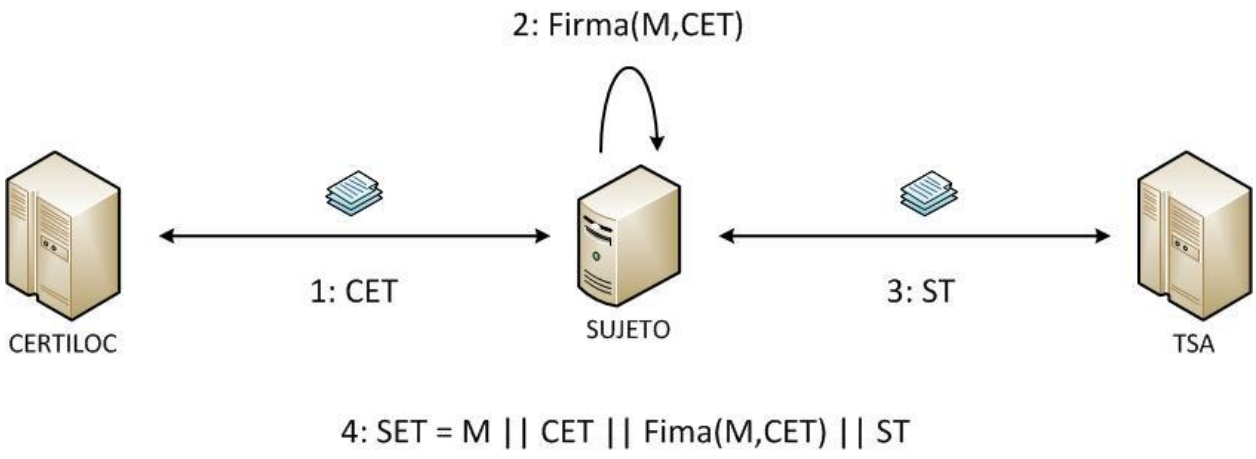


Ilustración 1 - Proceso de generación de un SET

Al finalizar este proceso se tiene un documento que establece que un Sujeto, localizado en un determinado lugar, realizó una firma digital en un determinado intervalo de tiempo (véase la Ilustración 2). El intervalo de tiempo viene determinado por los tiempos reflejados en el CET y en el ST. Y aunque no se pueda determinar con detalle el lugar exacto donde se realizó la firma, si se puede derivar con cierta seguridad la zona donde pudo ser generada la firma, dado que se conoce una posición inicial del sujeto (reflejada en el CET) y se puede asumir que se desplaza a cierta velocidad (actualmente, es razonable asumir, así mismo, que no va a poder desplazarse más rápidamente de lo establecido en las leyes de la física).

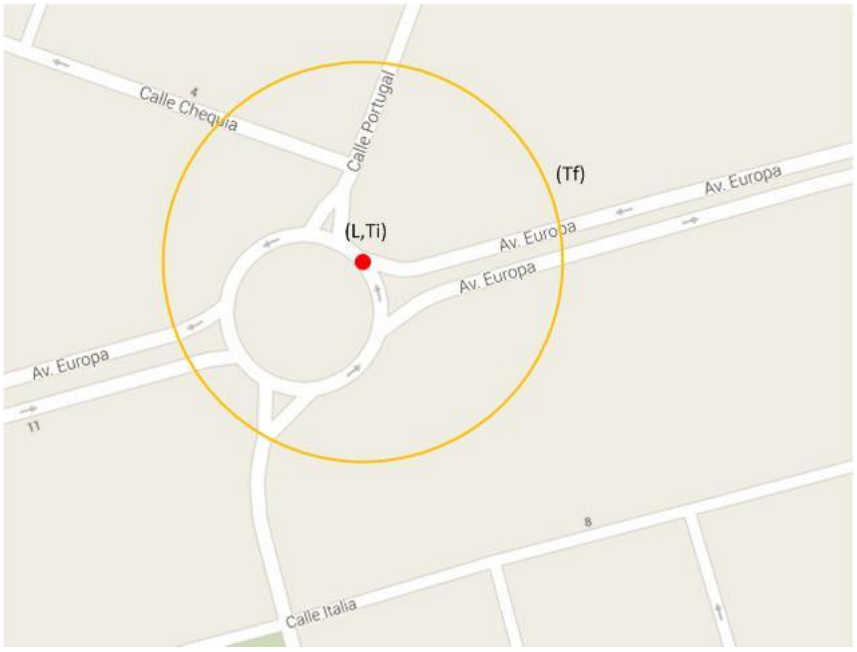


Ilustración 2 - Área de generación de la firma derivada de la información almacenada en un SET

Dos Proyectos Fin de Carrera previos a éste TFG abordan esta funcionalidad en el ámbito del proyecto CERTILOC. Dichos proyectos son los de Álvaro Gascón y Marín [2] y Raúl Calmaestra [1]. El primero de ellos consiste en una primera aproximación a la generación/validación de un SET y es en el segundo donde ya se implementa un sistema completo con todas las funcionalidades y características requeridas. En ambos proyectos se utiliza un simulador de CERTILOC en vez del propio demostrador desarrollado en [4], [5], [6] y [7], ya que dicho sistema necesita diversas actualizaciones para poder ser utilizado sin suponer riesgos de seguridad.

A fin de ilustrar brevemente cuál es el resultado final del sistema desarrollado en [1], se presentan unas capturas de pantalla de la interfaz del Sujeto (Ilustración 3) y del volcado e interpretación que hace dicho sistema de la información contenida en el SET por pantalla (Ilustración 4).

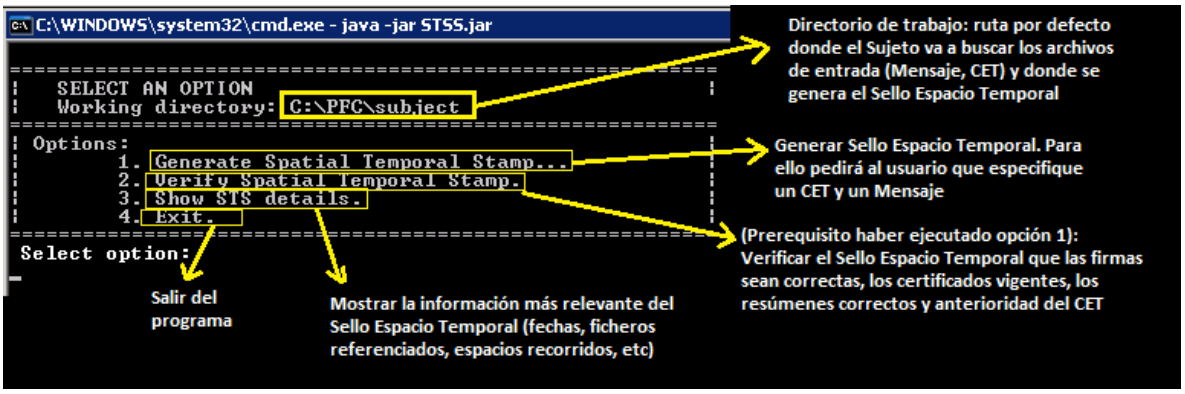


Ilustración 3 - Menú de opciones de [1].

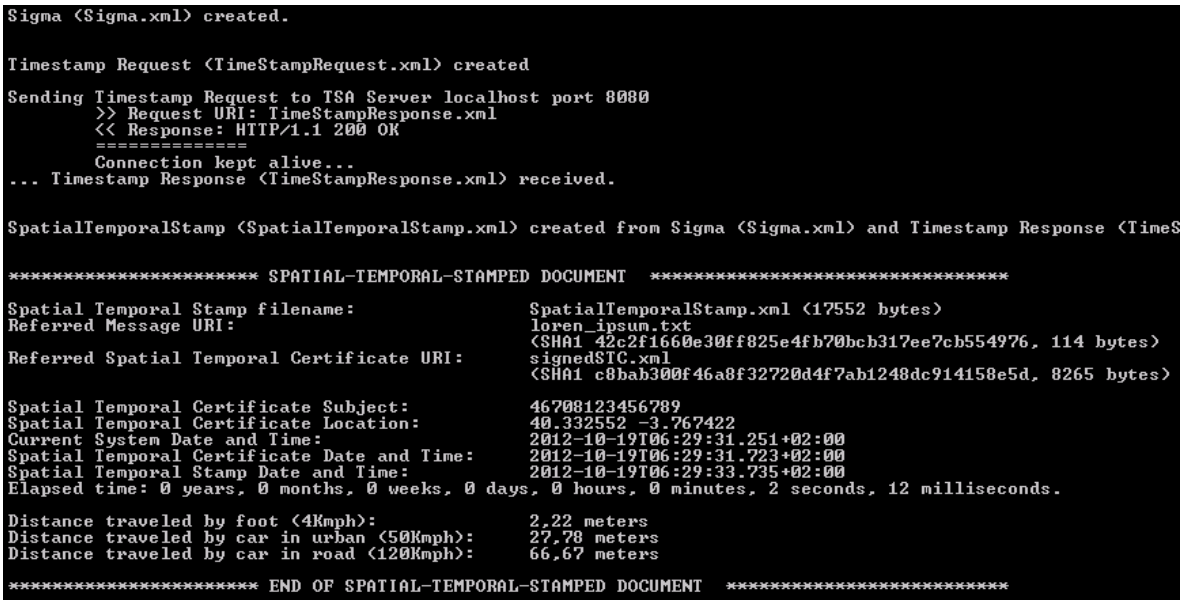


Ilustración 4 - Proceso de generación de un SET en [1].

1.2. Objetivos del TFG

Como se mencionó con anterioridad, el objetivo del presente TFG es la **adaptación del módulo cliente (SUBJECT) desarrollado en [1] a un dispositivo móvil**. Dado que es el primer trabajo que aborda la migración de dicho cliente a una plataforma móvil (en concreto, a un móvil con un sistema operativo Android), el alcance del TFG se limita a obtener un cliente con las mismas funcionalidades (o equivalentes) a las ofrecidas por el cliente en [1]. Por esa razón no se considera dentro del alcance del proyecto los siguientes asuntos:

- Comunicaciones seguras (ej., utilizando HTTPS) entre el cliente y los diferentes servicios (CERTILOC, TSA, DSS, TESTER). Es necesario mencionar que este requisito tampoco estaba contemplado en los proyectos fin de carrera [1] y [2] de los que parte este proyecto.
- Autenticación del cliente ante el servidor DSS, gestión de los certificados de firma del cliente por parte del DSS, así como inclusión en la firma digital generada de alguna prueba criptográfica que permita verificar a un tercero que el cliente solicitó dicho servicio. Estos requisitos vendrían derivados de la

utilización de un servicio de DSS, que hasta ahora no ha sido utilizado en CERTILOC.

Además, el cliente desarrollado en el TFG deberá disponer de una **interfaz gráfica** adecuada a un dispositivo móvil, similar a las ofrecidas por las aplicaciones actuales disponibles en el mercado.

1.3. Estructura del Documento

En este apartado se realizará una breve descripción de los diversos capítulos que componen este documento.

Introducción

Este capítulo describe el contexto global del proyecto CERTILOC y los objetivos a conseguir en este TFG, así como las motivaciones que han llevado a cabo la realización del mismo.

Gestión del Proyecto.

En este capítulo se describe la metodología utilizada para abordar el proyecto, la planificación prevista para su realización y el análisis de sus costes.

Estado de la Cuestión.

Este capítulo expone el ámbito de aplicación del presente documento y los conocimientos previos necesarios para la realización del mismo.

Análisis del Sistema

En este capítulo se expone el estudio realizado sobre los objetivos del proyecto, los problemas surgidos en la realización del mismo y solución propuesta.

Diseño e Implementación

Este capítulo incluye la descripción gráfica y textual de los diversos módulos software que componen el sistema así como su proceso de implementación.

Pruebas

En este capítulo se detallan las distintas pruebas realizadas para asegurar la calidad del software desarrollado y asegurar su buen funcionamiento.

Conclusiones y Líneas Futuras

Este capítulo expone las conclusiones finales del proyecto, explicando las dificultades encontradas durante su desarrollo y el resultado obtenido, y las líneas futuras de trabajo que se plantean.

Bibliografía.

En este capítulo aparecen todos los documentos, tesis doctorales, proyectos o páginas web que han sido necesarias para la realización de este proyecto.

Anexos.

Este apartado incluye un manual de usuario y manual de instalación del software desarrollado en el proyecto.

1.4. Definiciones

Resumen criptográfico: característica de un conjunto de datos, como el valor obtenido al aplicarlos una función resumen, tal que es computacionalmente inviable encontrar otro conjunto de datos que posea la misma característica.

Función resumen: función matemática que transforma valores de un conjunto grande en un conjunto de valores más pequeño.

Clave criptográfica: parámetro usado por un algoritmo para validar, autenticar, cifrar o descifrar un mensaje.

Clave pública: clave criptográfica de un usuario solo conocida por el mismo.

Clave pública: clave criptográfica de un usuario que se hace de público conocimiento.

Firma digital: datos añadidos a un conjunto de datos, o transformación de estos, que permite al receptor probar el origen e integridad del conjunto de datos recibidos, así como protegerlos contra falsificaciones.

Certificado de clave pública: clave pública de un usuario, junto con alguna otra información adicional, que se hace infalsificable cifrándola con la clave privada de la Autoridad de Certificación que las emite.

Autoridad de Certificación: autoridad confiable para uno o más usuarios que crea y asigna certificados.

Tercera Parte Fiable (Trusted Third Party, TTP): autoridad de seguridad, o agente suyo, confiable para otras entidades con respecto a actividades relativas a la seguridad.

Autenticación: proceso ejecutado entre un emisor y un receptor de un canal de transmisión para garantizar la integridad de los datos y la autenticidad del origen de los mismos.

Integridad: prevención de la modificación no autorizada de la información.

No repudio: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

Certificado Espacio-Temporal (CET): certificado que asocia a un usuario a un determinado lugar en un cierto momento.

Sellos de Tiempo (Time Stamp, ST): aserciones electrónicas sobre la presentación de un documento ante la TSA en un cierto momento.

Autoridad de Sellado-Temporal (Time Stamping Authority, TSA): TTP que emite sellos de tiempo.

Sello Espacio-Temporal (SET): acreditación que da fe de las condiciones espacio-temporales de un sujeto al realizar una firma digital sobre un documento.

2. GESTIÓN DEL PROYECTO

En este capítulo se expone la planificación, organización y administración de los recursos necesarios para finalizar el trabajo dentro de los márgenes de tiempo y coste definidos. En primer lugar se detallará la planificación del trabajo y la gestión de los riesgos que pudieran aparecer. Posteriormente, se indicarán los medios técnicos y económicos necesarios para la finalización del proyecto.

2.1. Planificación del Trabajo

En este apartado se expondrá la planificación temporal del proyecto. No obstante, como el proyecto tuvo que volver a ser planificado a mitad del mismo, se mostrarán dos diagramas: uno con la planificación inicial y otro con el desarrollo final realizado.

2.1.1. Ciclo de Vida

El ciclo de vida seleccionado para el proyecto es *desarrollo en cascada con retroceso o retroalimentación* (ver ilustración 5). Su modelo de trabajo es exactamente igual al *desarrollo en cascada* (de secuencia lineal) pero los retrocesos facilitan la solución de los fallos ocasionados en las fases finales del proyecto, pues nos permiten volver a cualquier fase anterior sin tener que reorganizar el proyecto.

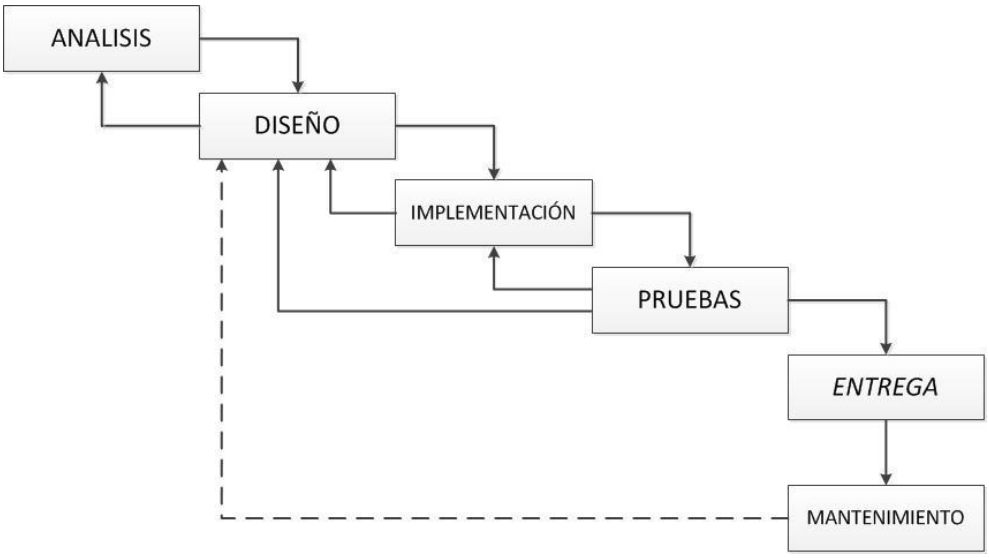


Ilustración 5 - Ciclo de vida del proyecto

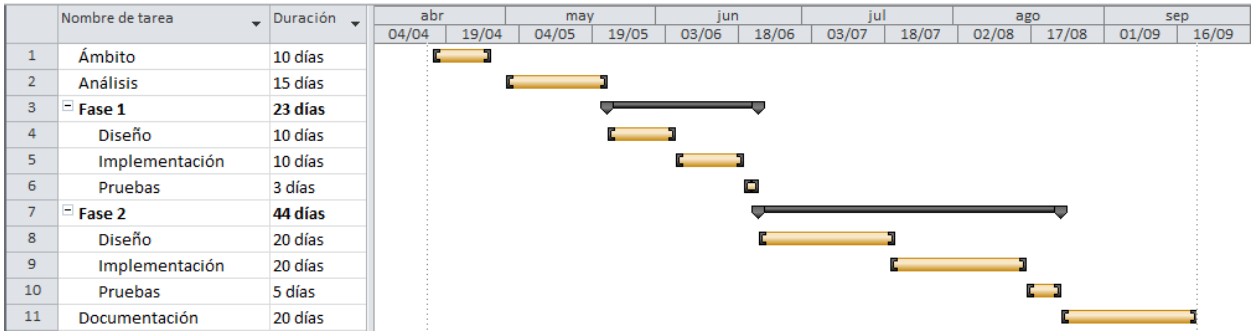
2.1.2. Planificación inicial

El periodo de desarrollo del presente proyecto comprende desde enero hasta septiembre de 2013. No obstante, debido a la finalización de los estudios académicos del autor, los primeros meses se planificaron como fases extensas.

El código del sistema desarrollado en [1] posee una estructura demasiado compleja para ser desplegado directamente como una aplicación móvil, y por esta razón se decidió plantear inicialmente el desarrollo de este TFG en las dos fases siguientes:

- Fase 1: simplificación del cliente desarrollado en [1] un entorno Java Eclipse para facilitar su posterior despliegue en un dispositivo con capacidades más limitadas.
- Fase 2: migración a dispositivo Android del resultado de la Fase 1.

La Ilustración 6 muestra la planificación inicial del proyecto. Se decidió planificar un mayor tiempo de desarrollo a la Fase 2, pues se consideraba de mayor dificultad la programación de una aplicación en un dispositivo Android que la simplificación de un código Java.



	Nombre de tarea	Duración
1	Ámbito	10 días
2	Análisis	15 días
3	**Fase 1**	**23 días**
4	Diseño	10 días
5	Implementación	10 días
6	Pruebas	3 días
7	**Fase 2**	**44 días**
8	Diseño	20 días
9	Implementación	20 días
10	Pruebas	5 días
11	Documentación	20 días

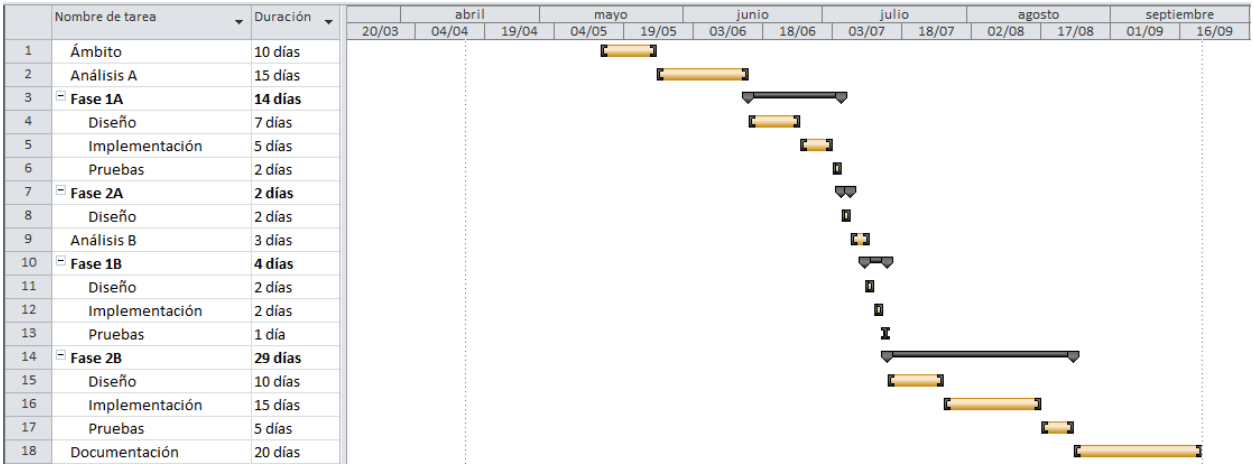
Ilustración 6 - Planificación inicial del proyecto

2.1.3. Desarrollo real del Proyecto

Una vez expuesta la planificación inicial, se mostrará el tiempo real que ha necesitado el proyecto para ser desarrollado (véase la Ilustración 7).

A primera vista se observa el retraso de aproximadamente un mes que se ha producido en el inicio del proyecto. A partir de la fecha de inicio, la planificación inicial para las fases de Ámbito y Análisis se ha cumplido.

Sin embargo, las dificultades encontradas en la Fase 2 supusieron la necesidad de realizar un nuevo diseño del sistema considerando la integración de una nueva entidad (servicio DSS). El diseño y desarrollo de este sistema revisado (con una nueva arquitectura) provocó cambios en la planificación inicial. En la Ilustración 7 se puede ver la planificación final acometida en el proyecto, donde se marcan con una A las fases del planteamiento inicial del sistema (Análisis A y fases 1A y 2A) y con una B las fases del sistema revisado (Análisis B y fases 1B y 2B), para diferenciar claramente ambas en el diagrama. No obstante, abordar de nuevo las dos fases para el sistema revisado no supuso un retraso muy grande debido al tiempo ganado anteriormente y a que el cambio a realizar en la arquitectura del sistema no era exageradamente grande.



	Nombre de tarea	Duración
1	Ámbito	10 días
2	Análisis A	15 días
3	**Fase 1A**	**14 días**
4	Diseño	7 días
5	Implementación	5 días
6	Pruebas	2 días
7	**Fase 2A**	**2 días**
8	Diseño	2 días
9	Análisis B	3 días
10	**Fase 1B**	**4 días**
11	Diseño	2 días
12	Implementación	2 días
13	Pruebas	1 día
14	**Fase 2B**	**29 días**
15	Diseño	10 días
16	Implementación	15 días
17	Pruebas	5 días
18	Documentación	20 días

Ilustración 7 - Calendario final del proyecto

2.2. Gestión de los Riesgos

Un riesgo es un posible o potencial daño para las unidades y/o personas que forman parte del desarrollo del proyecto. Se deben determinar los riesgos más frecuentes de ocurrir y los que más posibilidades tienen de afectar al proyecto para realizar una correcta gestión de los mismos y disponer de un plan ante ellos.

2.2.1. Fuente de los riesgos

Es necesario conocer el origen de los riesgos para poder analizarlos correctamente y definir la prevención adecuada para cada tipo de riesgo. A continuación se muestra el estudio realizado sobre ello:

- Internos: aquellos cuyo origen es el propio proyecto o los miembros de trabajo del mismo. Ej.: falta de conocimiento, problemas en fase de diseño, baja laboral…
- Externos: aquellos que provienen de un área diferente al ámbito del proyecto y grupo de trabajo. Ej.: problemas con el cliente, catástrofes naturales, perdida de material…

2.2.2. Parámetros de los riesgos

Para cada riesgo hallado, se definen los siguientes parámetros para explicar mejor su estudio y su contingencia:

- Probabilidad: indica la posibilidad de que el riesgo aparezca a lo largo del ciclo de vida del proyecto. Se le asignará un valor en la siguiente escala: *muy alta, alta, media, baja, muy baja*.
- Impacto: indica el daño que el riesgo puede causar al proyecto. Se delimitará una escala de tres valores para cuantificar el daño: *alto*, *medio* y *bajo*.
- Prioridad: indica la urgencia con la que el riesgo debe ser tratado. Se utiliza la escala numérica [1-5] para contabilizarla: siendo 5 la de mayor prioridad.

2.2.3. Identificación de los riesgos

A continuación se muestra el resultado del estudio realizado de los riesgos, así como sus consecuencias, contingencias y medidas de sus parámetros.

R001	
Descripción	Baja temporal de un miembro del grupo de trabajo.
Causa	Enfermedad.
Consecuencia	Retrasos en la planificación.
Origen	Interno.
Impacto	Alto.
Probabilidad	Media.
Prioridad	4
Prevención	Se realizarán controles médicos periódicos hasta la finalización del proyecto.
Contingencia	No existen recursos humanos adicionales.

Tabla 1 - R001: Baja temporal de un miembro del grupo de trabajo

R002	
Descripción	Baja definitiva de un miembro del grupo de trabajo.
Causa	Fallecimiento, retirada del proyecto.
Consecuencia	Cancelación del proyecto.
Origen	Interno.
Impacto	Alto.
Probabilidad	Muy baja.
Prioridad	5
Prevención	Se realizarán controles médicos periódicos hasta la finalización del proyecto.
Contingencia	No existen recursos humanos adicionales.

Tabla 2 - R002: Baja definitiva de un miembro del grupo de trabajo

R003	
Descripción	Falta de colaboración del cliente.
Causa	Desinterés, falta de tiempo…
Consecuencia	Retraso en la planificación.
Origen	Externo.
Impacto	Alto.
Probabilidad	Baja.
Prioridad	4
Prevención	Planificar reuniones con el cliente a lo largo del proyecto.
Contingencia	Avanzar partes del proyecto que no necesiten intervención del cliente.

Tabla 3 - R003: Falta de colaboración del cliente

R004	
Descripción	Un miembro del equipo no tiene la formación adecuada.
Causa	Falta de formación
Consecuencia	Retraso en la planificación.
Origen	Interno.
Impacto	Alto.
Probabilidad	Baja.
Prioridad	4
Prevención	Realizar cursos antes de emprender las tareas del proyecto.
Contingencia	Replanificar tareas y adquirir la formación necesaria.

Tabla 4 - R004: Un miembro del equipo no tiene la formación adecuada

R005	
Descripción	Eliminación de datos del proyecto por parte de un miembro.
Causa	Falta de atención
Consecuencia	Retraso en la planificación.
Origen	Interno.
Impacto	Alto.
Probabilidad	Baja.
Prioridad	5
Prevención	Realizar copias de seguridad del proyecto.
Contingencia	Restaurar la última copia de seguridad.

Tabla 5 - R005: Eliminación de datos del proyecto por parte de un miembro

R006	
Descripción	Errores en la estimación de la planificación del proyecto.
Causa	Falta de experiencia.
Consecuencia	Retraso en la planificación y aumento de costes.
Origen	Interno.
Impacto	Alto.
Probabilidad	Media.
Prioridad	4
Prevención	Basar la estimación en las planificaciones de proyectos anteriores similares al actual.
Contingencia	Reestimar la magnitud del proyecto.

Tabla 6 - R006: Errores en la estimación de la planificación del proyecto

R007	
Descripción	Un equipo tiene un fallo en uno de sus componentes.
Causa	Fallo en hardware.
Consecuencia	Retraso en la planificación y aumento de costes.
Origen	Interno.
Impacto	Medio.
Probabilidad	Muy baja.
Prioridad	3
Prevención	Comprobar que los equipos funcionan correctamente antes de iniciar el proyecto.
Contingencia	Sustituir la pieza dañada.

Tabla 7 - R007: Un equipo tiene un fallo en uno de sus componentes

R008	
Descripción	Cambio de los requisitos por parte del cliente.
Causa	Cambio de idea del cliente.
Consecuencia	Replanificación del proyecto y revisión del trabajo.
Origen	Externo.
Impacto	Alto.
Probabilidad	Baja.
Prioridad	4
Prevención	Realizar reuniones con el cliente para asegurar que el proyecto sigue lo planificado.
Contingencia	Continuar el trabajo que no se haya visto afectado y planificar los nuevos cambios.

Tabla 8 - R008: Cambio de los requisitos por parte del cliente

R009	
Descripción	Incendio en la zona de producción/implantación.
Causa	Negligencia, fallo eléctrico…
Consecuencia	Perdida material, retraso en la planificación y aumento de costes.
Origen	Externo.
Impacto	Alto.
Probabilidad	Muy baja.
Prioridad	5
Prevención	Almacenar información y copias de respaldo fuera de los entornos de producción e implantación.
Contingencia	Reparar el material dañado y restaurar los datos perdidos.

Tabla 9 - R009: Incendio en la zona de producción/implantación

R010	
Descripción	Inundación en la zona de producción/implantación.
Causa	Negligencia o catástrofe natural.
Consecuencia	Perdida material, retraso en la planificación y aumento de costes.
Origen	Externo.
Impacto	Alto.
Probabilidad	Muy baja.
Prioridad	5
Prevención	Almacenar información y copias de respaldo fuera de los entornos de producción e implantación.
Contingencia	Reparar el material dañado y restaurar los datos perdidos.

Tabla 10 - R010: Inundación en la zona de producción/implantación

R011	
Descripción	Subida de tensión en la zona de producción/implantación.
Causa	Negligencia o errores en la compañía eléctrica.
Consecuencia	Perdida de información.
Origen	Externo.
Impacto	Alto.
Probabilidad	Muy baja.
Prioridad	5
Prevención	Almacenar información y copias de respaldo fuera de los entornos de producción e implantación.
Contingencia	Restaurar los datos perdidos.

Tabla 11 - R011: Subida de tensión en la zona de producción/implantación

R012	
Descripción	Corte de suministro eléctrico.
Causa	Negligencia o errores en la compañía eléctrica.
Consecuencia	Perdida eventual de información.
Origen	Externo.
Impacto	Alto.
Probabilidad	Muy baja.
Prioridad	5
Prevención	Almacenar información y copias de respaldo fuera de los entornos de producción e implantación.
Contingencia	Restaurar los datos perdidos.

Tabla 12 - R012: Corte de suministro eléctrico

R013	
Descripción	Robos de material.
Causa	Fallos de seguridad.
Consecuencia	Perdida material, retraso en la planificación y aumento de costes.
Origen	Externo.
Impacto	Medio.
Probabilidad	Muy baja.
Prioridad	4
Prevención	Almacenar información y copias de respaldo fuera de los entornos de producción e implantación.
Contingencia	Reponer el material robado y restaurar los datos perdidos.

Tabla 13 - R013: Robos de material

R014	
Descripción	Virus o ataque informático.
Causa	Fallos de seguridad en los equipos.
Consecuencia	Perdida de información.
Origen	Externo.
Impacto	Medio.
Probabilidad	Muy baja.
Prioridad	4
Prevención	Almacenar información y copias de respaldo fuera de los entornos de producción e implantación.
Contingencia	Restaurar los datos perdidos.

Tabla 14 - R014: Virus o ataque informático

R015	
Descripción	El presupuesto es insuficiente.
Causa	Error en la estimación de costes.
Consecuencia	Fracaso del proyecto o finalización con pérdidas.
Origen	Interno
Impacto	5
Probabilidad	Baja.
Prioridad	5
Prevención	Basarse en proyectos anteriores para planificar los presupuestos.
Contingencia	Continuar las partes no afectadas y replanificar el presupuesto.

Tabla 15 - R015: El presupuesto es insuficiente

R016	
Descripción	Cancelación del proyecto.
Causa	Gestión inadecuada o finalización por parte del cliente.
Consecuencia	Fin del proyecto.
Origen	Interno o Externo
Impacto	5
Probabilidad	Muy baja.
Prioridad	4
Prevención	No es posible prevenir este riesgo.
Contingencia	No es posible contener este riesgo.

Tabla 16 - R016: Cancelación del proyecto

2.3. Medios Técnicos

A continuación se va a enumerar los elementos hardware y software que se han utilizado durante las distintas fases del proyecto:

Hardware Ordenador Intel® Core™ i5 a 3.20GHz con 16Gb de RAM y 500Gb HD.

Ordenador Toshiba Portege Z830.

Teléfono móvil Samsung Galaxy S II.

Impresora HP LaserJet 4L.

Software Microsoft® Windows 7 Professional.

Microsoft® Office 2010.

Microsoft® Visio 2010.

Microsoft® Project 2010.

Eclipse SDK 4.2.2

JDK 7

StarUML

2.4. Análisis Económico

En este apartado se indica el análisis económico del proyecto, donde se estimarán los costes necesarios con el fin de cuantificar los beneficios y la inversión inicial necesaria para el desarrollo del proyecto. Los costes del proyecto vendrán derivados de los siguientes recursos:

- **Recursos humanos**: el coste de las horas que cada trabajador debe emplear al proyecto en sus distintas fases.
- **Recursos hardware**: el coste del material hardware indicado en el apartado anterior.
- **Recursos software**: el coste del material software indicado en el apartado anterior.
- **Recursos fungibles**: el coste de material de oficina, cartuchos de tinta…

2.4.1. Coste de personal

En la tabla 17 se puede ver el coste del personal que ha participado en el proyecto. Para realizar el cálculo de costes de esta sección, se han tenido en cuenta el trabajo de un Ingeniero Informático como ingeniero desarrollador. Dicho coste está calculado por horas, estimando 8 horas por día de trabajo, e incluye los gastos en concepto de Seguridad Social (20%):

ROL	Horas Estimadas	Coste (€/hora)	Coste Total
Ámbito y Análisis	200	24	4800
Diseño	240	18	4320
Implementación	240	14,4	3456
Pruebas	64	12	768
Documentación	120	12	1920
TOTAL COSTE PERSONAL			**15264 €**

Tabla 17 - Coste de personal imputable al proyecto

2.4.2. Costes de hardware

En la tabla 18 se detallan los costes del equipo hardware estimado para la realización del proyecto, incluyendo su amortización:

Hardware	Coste sin I.V.A (€)	Vida útil estimada (meses)	Tiempo de uso en proyecto (meses)	Coste imputable al proyecto (€)
Intel® Core™ i5 a 3.20 GHz, 16 Gb RAM, 500 Gb. HD	2487,60	48	5	259,13
Toshiba Portege Z830.	825,62	36	5	114,67
Smatphone Android.	431,03	36	5	59,87
Impresora HP LaserJet 4L.	100,8	36	5	14
TOTAL COSTE HARDWARE				447,66 €

Tabla 18 - Coste de hardware imputable al proyecto

2.4.3. Costes de software

En la tabla 19 se detallan los costes del material software estimado para la realización del proyecto, incluyendo su amortización:

Software	Coste sin I.V.A (€)	Duración de la licencia (meses)	Tiempo de uso en proyecto (meses)	Coste imputable al proyecto (€)
Microsoft® Windows 7 Professional.	186,22	Indefinida (estimada 48)	5	19,40
Microsoft® Office 2010.	98,35	Indefinida (estimada 48)	5	10,24
Microsoft® Visio 2010.	0 (licencia MSDN)	Indefinida	5	0
Microsoft® Project 2010.	0 (licencia MSDN)	Indefinida	5	0
Eclipse SDK 4.2.2	0	Indefinida	5	0
JDK 7	0	Indefinida	5	0
StarUML	0	Indefinida	5	0
TOTAL COSTE SOFTWARE				**29,64 €**

Tabla 19 - Costes de software imputados al proyecto

2.4.4. Costes de recursos fungibles

En estos recursos se contabiliza los materiales de oficina habituales: bolígrafos, folios, lápices, cartuchos de tinta… De acuerdo a las necesidades del proyecto, se estima un coste total de 100€ para estos recursos.

2.4.5. Resumen de costes y presupuesto

En la tabla 20 se puede ver un resumen del coste total de todos los recursos:

Concepto	Coste sin I.V.A (€)
Recursos Humanos	15264
Recursos Hardware	447,66
Recursos Software	29,64
Recursos Fungibles	100
Total Costes Directos (TCD)	15841,30
Costes Indirectos (15% TCD)	2376,20
COSTE TOTAL (sin I.V.A)	**18217,50**

Tabla 20 - Total de costes

Para la realización de un presupuesto de venta, se debe garantizar un margen de beneficio económico del proyecto. Por lo tanto, se debe cuantificar un margen de riesgo y un porcentaje de beneficio. En este proyecto, se utilizará un 15% de margen de riesgo y un beneficio económico del 20%

Concepto	Valor (€)
Costes de realización (sin I.V.A)	18217,50
Prima por riesgo (15%)	2732,62
Total Costes (sin I.V.A)	20950,12
Beneficio del Proyecto (20% costes)	4190,02
Precio de realización (sin I.V.A)	25140,14
I.V.A (21%)	5279,43
TOTAL	**30419,57**

Tabla 21 - Presupuesto para el cliente

El coste total del proyecto es de **30419,57 €** (treinta mil cuatrocientos diecinueve euros con cincuenta y siete céntimos).

3. ESTADO DE LA CUESTIÓN

En este capítulo realiza una breve exposición sobre las firmas digitales en dispositivos móviles, describiendo qué es una firma digital, el estándar de firma digital XMLDSig y cómo se utiliza este estándar en el sistema operativo Android y el servicio de firma digital DSS (Digital Signature Service). Finalmente, se llevará a cabo un breve resumen sobre el sistema desarrollado en [1].

3.1. Firmas digitales en dispositivos móviles

3.1.1. Qué es una firma digital

Una **firma digital** es un mecanismo criptográfico que permite a un sujeto firmar un mensaje y confirmar que él es el autor de dicho mensaje (autenticación y no repudio) y que no ha sido alterado desde que se realizó la firma (integridad) [15].

Una firma digital debe de ser equivalente a las firmas manuales, es decir, debe cumplir:

- Fácil y barata de producir.
- Fácil de reconocer.
- Imposible de rechazar por el propietario.
- Infalsificable (teóricamente): para falsificar una firma digital el atacante tiene que resolver problemas matemáticos de una complejidad muy elevada, es decir, las firmas han de ser computacionalmente seguras.
- Única: las firmas electrónicas no pueden ser siempre la misma ya que sería fácilmente falsificable.

Más técnicamente, la Ley 59/2003 [10] establece que la firma electrónica es "*el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante*". Uno de sus usos más extendidos es el

DNI electrónico, definido también en la misma ley como "*documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos*".

La firma digital permite detectar la manipulación o falsificación de contenidos, por lo que se utiliza de manera muy extendida. Sobre todo en campos donde es necesario verificar la autenticidad e integridad de los datos, como documentos electrónicos, comercio electrónico, software, etc.

3.1.2. El estándar de firma digital XMLDSig

Existen diversos estándares de firma digital. Algunos de ellos tienen su origen ligado a la invención de este mecanismo (PKCS#7 [24]), apareciendo el resto en los años siguientes. Los más conocidos a día de hoy, aparte del ya mencionado, son el RFC 2634 [25] y el ISO 9796-2 [26].

Con la aparición del XML es necesario proponer nuevos estándares para representar firmas digitales en documentos XML y además convenir cómo se deben generar y validar firmas sobre documentos o elementos XML. El estándar que se ha desarrollado para estas necesidades es el **XML Digital Signature Estándar** (**XMLDSig**), que es una recomendación del W3C [8] y una RFC del IETF [9]

Este estándar define una sintaxis XML para representar de firmas digitales así como los procedimientos para generarlas y validarlas. Esta especificación puede firmar cualquier elemento o conjunto de elementos accesibles a través de una dirección URL.

Dependiendo de si el contenido está dentro o fuera del documento que contiene la firma, la firma XML puede ser de dos tipos:

- Firma separada (*detached*): el elemento firmado está fuera del documento que contiene la firma.
- Firma envuelta (*enveloped*): el elemento firmado es parte del documento que contiene la firma.

- Firma envolvente (*enveloping*): la firma contiene los datos firmados dentro de sí mismo.

La estructura básica de la firma XML, con sus correspondientes elementos, definida por el W3C es la siguiente:

```
<Signature>
  <SignedInfo>
    <SignatureMethod />
    <CanonicalizationMethod />
    <Reference>
       <Transforms>
       <DigestMethod>
       <DigestValue>
    </Reference>
    <Reference /> etc.
  </SignedInfo>
  <SignatureValue />
  <KeyInfo />
  <Object />
</Signature>
```

Ilustración 8 - Estándar de firma XML

SignedInfo: contiene o referencia los datos firmados y especifica el algoritmo de firma.

SignatureValue: contiene el valor de la firma en Base64.

KeyInfo: certificados digitales X509 adicionales a la firma (opcional) o información que permite recuperar o identificar la clave pública del firmante.

Object: datos firmados en caso de ser una firma de tipo *enveloped*.

Las firmas digitales XML, a diferencia de las firmas digitales que se hacían anteriormente, tiene el problema de poseer una complejidad exponencial. Mientras que en los documentos XML se pueden modificar ciertas características de los nodos, elementos, atributos, la inclusión o no de los espacios de nombres o la adición de saltos de línea y comentarios sin que cambie la información que almacena, en las firmas digitales cualquier mínima modificación (a nivel de bit) supone la invalidación de la misma.

Por esta razón y para poder dar soporte a la flexibilidad ofrecida por XML, las firmas digitales XML contienen dos elementos que aumentan aún más su complejidad. Por un lado, el nodo <*CanonicalizationMethod*> indica el algoritmo que usa la firma para normalizar el elemento a firmar. Es decir, se modifica el elemento a firmar para que siga un estándar definido (es necesario para convenir exactamente qué se va a firmar a

partir de documentos XML que representan la misma información pero que podrían presentar diferencias a nivel de bit).

Por otro lado, el estándar XMLDSig da la opción de realizar transformaciones cuando las firmas son de tipo *detached*. Estas transformaciones pueden ser, por ejemplo, modificaciones de los bytes del documento antes de ser firmado o selección de subelementos concretos que satisfagan determinadas características. El algoritmo o algoritmos usados se almacenan en el nodo <*Transforms*>.

3.1.3. El sistema operativo Android, Java y las firmas digitales XMLDSig

A raíz del exponencial crecimiento de los dispositivos móviles, los sistemas operativos convencionales han necesitado ser modificados para poder ser utilizados en estos dispositivos. Aunque algunos han podido ser modificados para estos dispositivos (iOS o Windows Phone), se han desarrollado sistemas operativos exclusivos para dispositivos móviles (Android o Symbian OS) o los fabricantes de estos dispositivos han desarrollado sus propios sistemas operativos (BlackBerry OS).

A la hora de desarrollar una aplicación para un dispositivo móvil es necesario evaluar todos los sistemas operativos existentes en el mercado para que el alcance de la aplicación sea el mayor posible. Por ello, para el desarrollo de este TFG se ha elegido como sistema operativo Android, ya que posee la mayor cuota de mercado actual [21].

El sistema operativo Android fue diseñado principalmente para dispositivos móviles como tabletas o teléfonos inteligentes. Dicho sistema operativo está basado en Linux para el desarrollo de los servicios del sistema como seguridad, gestión de memoria, gestión de procesos, pila de red y modelo de controladores.

Android se desarrolla de forma abierta, permitiendo acceder a su código fuente de forma libre. Esto facilita el desarrollo de aplicaciones para este sistema operativo por parte de cualquier programador con conocimientos de Java, C o C++; aunque su implementación en Android no es exactamente igual a la que pudiera tener en un ordenador de sobremesa o portátiles. Por lo tanto, ya que el proyecto desarrollado en

[1] está programado en lenguaje Java, la elección del lenguaje de programación para este TFG será también Java, permitiendo así la reutilización de código.

Sin embargo, la versión de Java para Android no soporta todas las librerías o paquetes disponibles en dichos lenguajes de programación, lo que puede provocar problemas a la hora de desarrollar aplicaciones. Uno de esos paquetes no soportados es XMLSignature, perteneciente a la librería Apache Santuario [9]. Dicho paquete permite generar y validar la firma de un documento digital según el estándar XML Digital Signature [22], obteniendo integridad, no repudio y autenticación de la información almacenada en el documento.

Por otro lado, para la firma de un documento es necesario un par de claves privada/pública (recomendable que la clave pública esté certificada por una Autoridad de Certificación). Aunque Android no soporta los tipos de almacén de certificados más comúnmente utilizados (JKS, el utilizado en [1], o CRT), si soporta el formato BKS, por lo que podría utilizarse certificados de este tipo en las aplicaciones desarrolladas.

Dado que un requisito del proyecto es que el sujeto realice una firma digital XMLDSig a través de su dispositivo móvil, en caso de no ser posible utilizar una librería que ofrezca esta funcionalidad, se pueden considerar otras dos alternativas:

a) Implementar directamente la generación y validación de firmas digitales en XML sin utilizar librerías con este objetivo para su despliegue en el dispositivo móvil.

b) Utilizar un servicio de generación y validación de firmas digitales XML (externo al móvil). Estos servicios se conocen como Digital Signature Services y se describe brevemente la principal de sus especificaciones en la sección siguiente 3.1.4.

En el capítulo 4. Análisis del Sistema se exponen las razones para elegir la segunda alternativa.

3.1.4. Digital Signature Service (DSS)

Digital Signature Service es una especificación de OASIS (*Organization for the Advancement of Structured Information Standards*) que describe un protocolo cliente-servidor de petición y respuesta para la generación y validación de firmas digitales sobre documentos.

El protocolo (ver ilustración 9) define que un cliente puede enviar documentos a un servidor, que devolverá una firma de los mismos. Del mismo modo, el cliente podrá enviar documentos firmados para que el servidor le indique si las firmas son válidas o no.

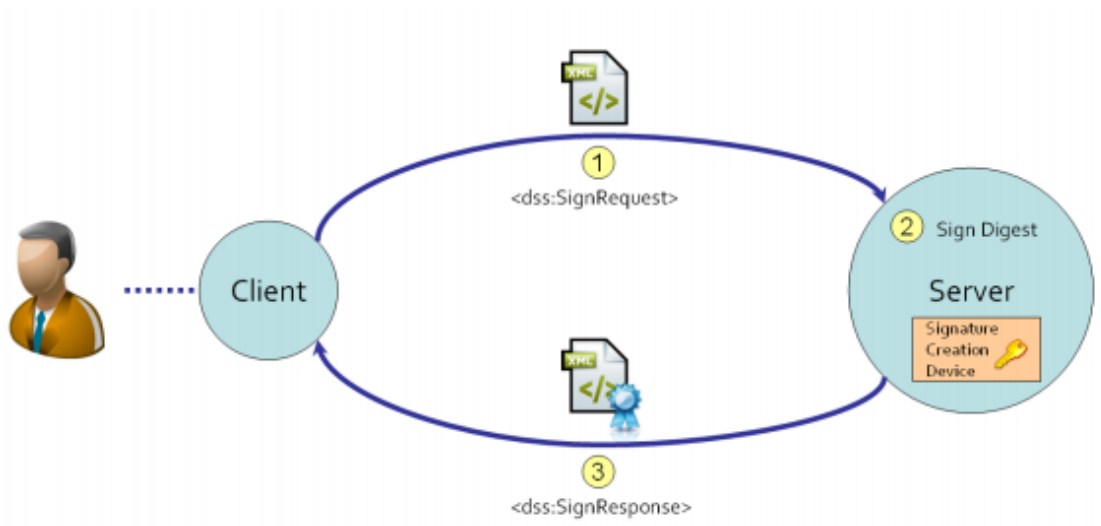


Ilustración 9 - DSS protocol

La especificación de OASIS no declara qué tipo de información debe contener la petición y respuesta, simplemente indica cómo ha de realizarse la conexión cliente-servidor dependiendo de la arquitectura del sistema (cliente remoto, dispositivo móvil, smartcard, etc.).

Actualmente existen varias empresas o servicios que proporcionan dicha funcionalidad de firma electrónica a través de servicios de firma digital (DSS), como Zylk.net, pero no existe ninguna librería gratuita que permita implementar este servicio en Java.

3.2. Servicio de sellado espacio-temporal de CERTILOC

El ámbito del proyecto de investigación CERTILOC requiere definir una metodología, protocolos e implementación de un sistema basado en la localización espacio temporal que provea servicios de seguridad sobre dicha información.

Como se indica en [1], *los objetivos del proyecto de investigación CERTILOC son, en primer lugar, plantear un modelo teórico que permita certificar la información espacio temporal de una determinada entidad y, en segundo lugar, implementar un demostrador que nos permita verificar y probar el funcionamiento de dicho modelo. Dicho demostrador ha sido desarrollado conjuntamente en una serie de proyectos y provee una serie de servicios de seguridad que en conjunto se denominan Servicios de Acreditación y Sellado Espacio Temporal (SASET):*

- *Servicio de acreditación Espacio-Temporal (SAET), cuyo objetivo es acreditar las condiciones espacio-temporales de una entidad o sujeto S de las evidencias. Las evidencias que emiten este tipo de servicios reciben el nombre de credenciales o Certificados Espacio Temporales (CET).*

- *Servicio de Sellado Espacio Temporal (SSET), cuyo objetivo es acreditar que un determinado documento (M) existía en un lugar determinado en cierto momento temporal o que un sujeto S realizó determinada acción sobre dicho documento bajo ciertas condiciones espacio-temporales. En este caso, las evidencias se denominan sellos espacios-temporales (SET).*

- *Servicio de Provisión de Privacidad del Usuario. En este sentido el demostrador tiene implementado un módulo que hace cumplir una serie de políticas de privacidad.*

En el trabajo desarrollado en [1] extiende la metodología, protocolos e implementación del sistema de localización espacio-temporal desarrollado en [2]. Dichos protocolos se basan en el uso de servicios de confianza provistos por unas entidades llamadas Terceros de Confianza (TTP, *Trusted Third Parties*).

Estas entidades actúan como intermediarias entre varias entidades, dando fe de la veracidad de la información proporcionada por una de ellas ante las demás; siendo necesario que tanto la parte emisora como las receptoras confíen en dicho Tercero de Confianza para que el sistema funcione correctamente Es decir, proporcionan confidencialidad, integridad y disponibilidad de la información. Algunos ejemplos de su uso son el comercio electrónico, el acceso a los datos bancarios, entidades de la administración pública o un elemento más cercano como el DNI electrónico.

En el apartado 1.1 Contexto: El Proyecto CERTILOC, se explicó brevemente qué es un SET y cómo se generan en CERTILOC. El SET determina la posición de S, pues dispone de una localización espacial inicial (almacenada en el certificado) y un intervalo de tiempo (entre la generación del certificado y el sello temporal) mediante los cuales se puede determinar la posible área donde S generó la firma digital.

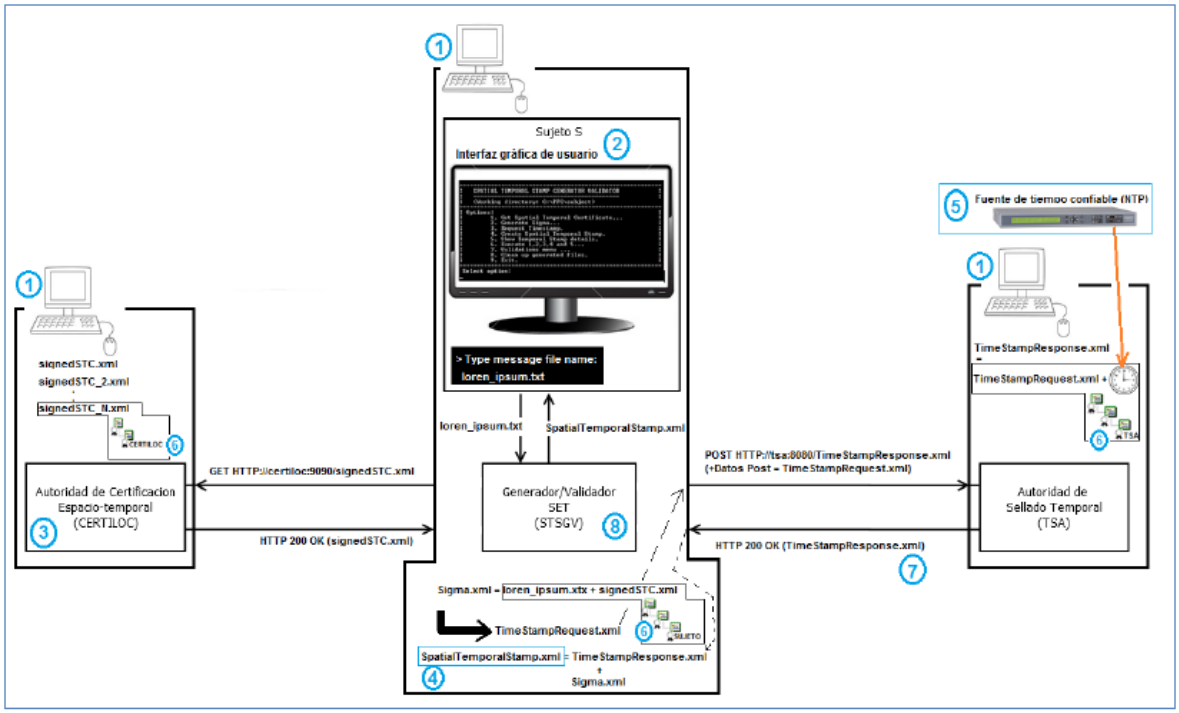


Ilustración 10 - Generación del sello espacio-temporal de CERTILOC

En el sistema desarrollado en [1] se dispone de 3 entidades: SUBJECT, que es quien genera las firmas; CERTILOC, que proporciona un CET sobre SUBJECT; y TSA, que proporciona un ST, que junto al CET, acotan a SUBJECT en una determinada zona dependiendo del tiempo transcurrido entre ambos.

Dicho sistema opera de la siguiente manera (véase la Ilustración 11):

1. SUBJECT solicita un certificado espacio-temporal a CERTILOC.
2. CERTILOC envía el certificado a SUBJECT.
3. SUBJECT genera Sigma, que es la firma digital sobre el certificado y el documento que se desea firmar.
4. SUBJECT genera una solicitud de emisión de un sello temporal sobre Sigma (*TimeStampRequest*) y lo envía a TSA.
5. TSA genera un el sello temporal solicitado y lo envía a SUBJECT (*TimeStampResponse*).
6. SUBJECT genera el sello espacio-temporal (*SpatialTemporalStamp*) uniendo el CET, el documento M, la firma Sigma y el sello temporal contenido en *TimeStampResponse*.

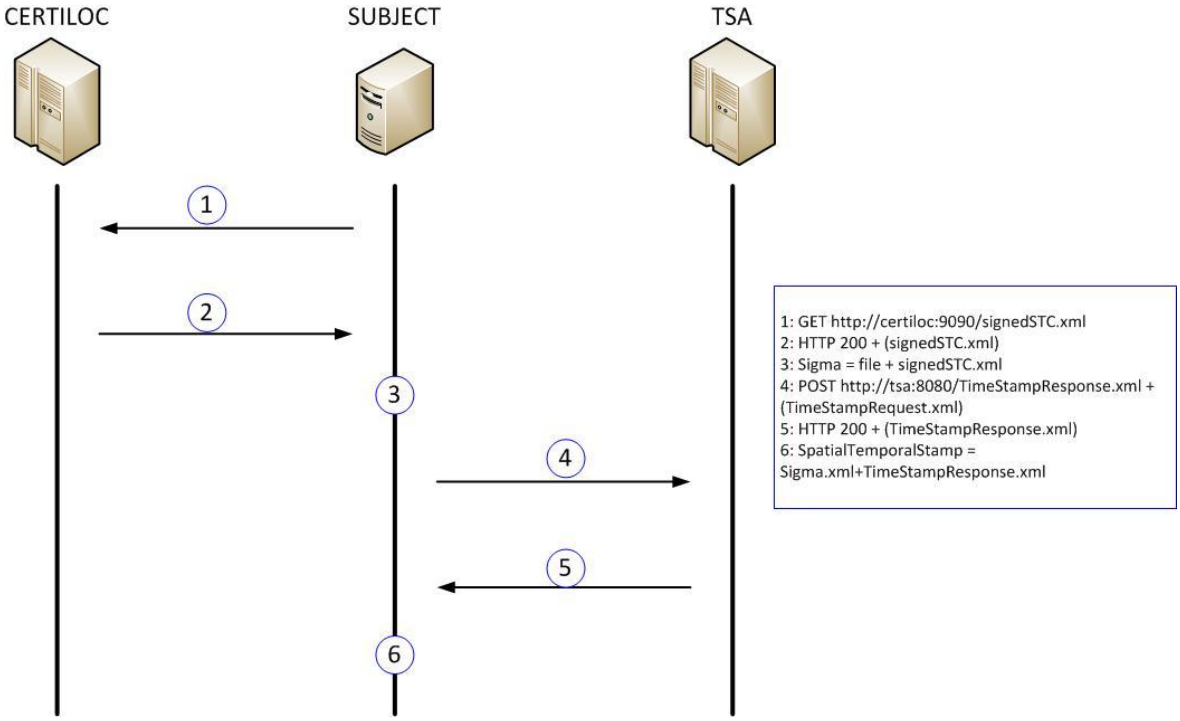


Ilustración 11 - Arquitectura de [1]

En las siguientes imágenes se pueden ver la interfaz de las entidades de [1]: la entidad SUBJECT (ver ilustración 12), la entidad CERTILOC (ver ilustración 13) y la entidad TSA (ver ilustración 14).

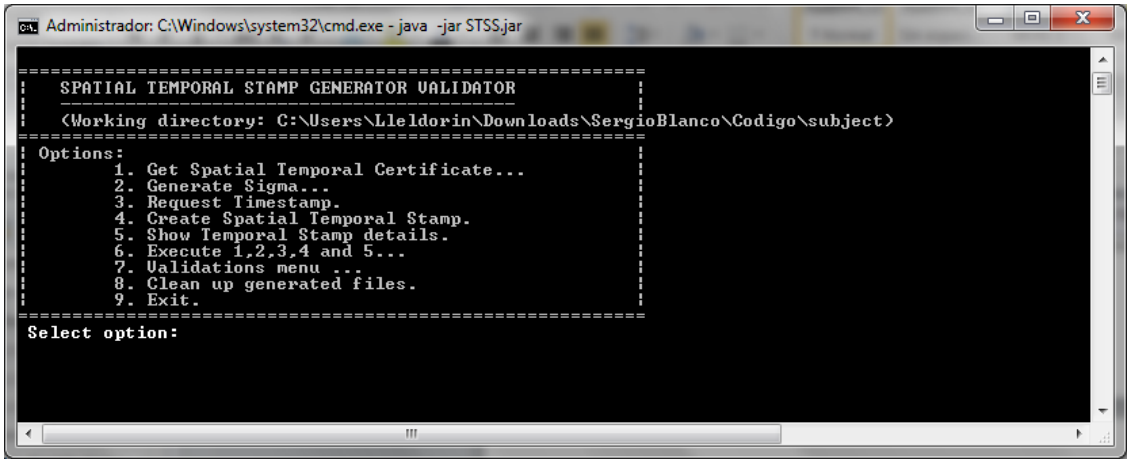


Ilustración 12 - Interfaz del módulo cliente de [1]

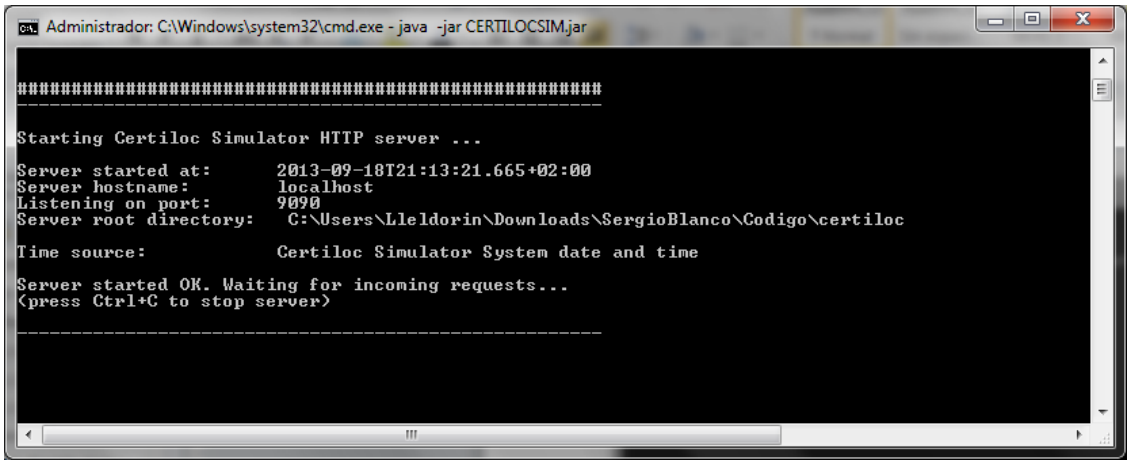


Ilustración 13 - Interfaz del módulo CERTILOC de [1]

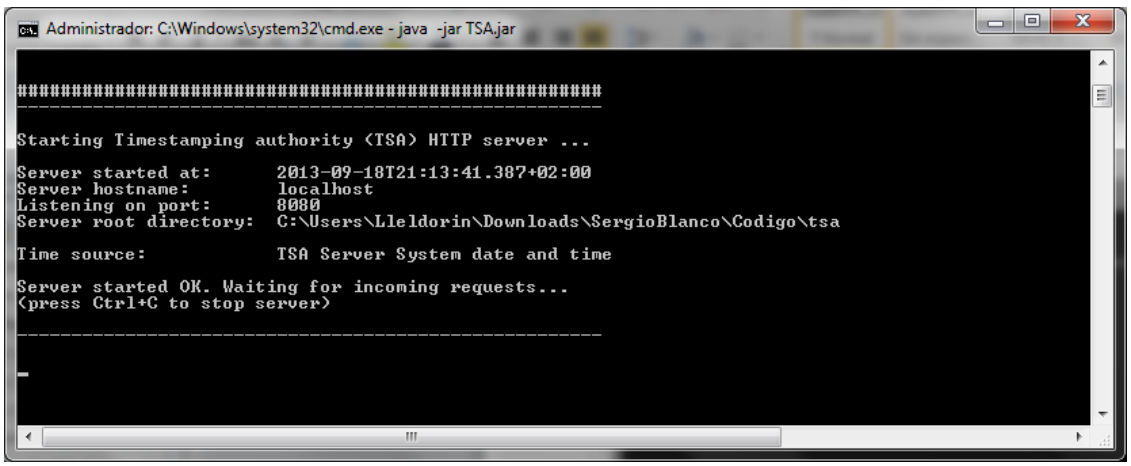
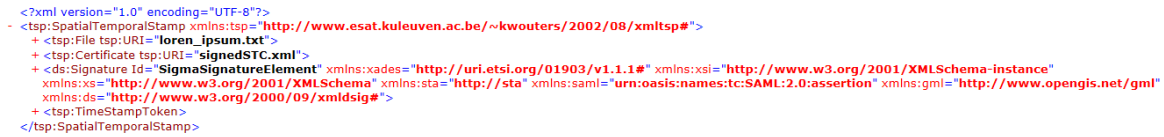


Ilustración 14 - Interfaz del módulo TSA en [1]

A continuación, se muestra el SET resultante al finalizar el proceso de generación de [1]. Primeramente se mostrarán los principales elementos del SET (ver ilustración 15). Seguidamente se mostrarán los elementos que hacen referencia al documento M, al CET y la firma Sigma (ver ilustración 16) y, finalmente, se mostrará el sello temporal (ver ilustración 17).



```
<?xml version="1.0" encoding="UTF-8"?>
- <tsp:SpatialTemporalStamp xmlns:tsp="http://www.esat.kuleuven.ac.be/~kwouters/2002/08/xmltsp#">
  + <tsp:File tsp:URI="loren_ipsum.txt">
  + <tsp:Certificate tsp:URI="signedSTC.xml">
  + <ds:Signature Id="SigmaSignatureElement" xmlns:xades="http://uri.etsi.org/01903/v1.1.1#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:sta="http://sta" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:gml="http://www.opengis.net/gml"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  + <tsp:TimeStampToken>
  </tsp:SpatialTemporalStamp>
```


Ilustración 15 - Elementos de SpatialTemporalStamp generado en [1]

```
<?xml version="1.0" encoding="UTF-8"?>
- <tsp:SpatialTemporalStamp xmlns:tsp="http://www.esat.kuleuven.ac.be/~kwouters/2002/08/xmltsp#">
  - <tsp:File tsp:URI="loren_ipsum.txt">
    - <tsp:DigestAlgValue Id="HEX(SHA-1(Message file)">
        <xades:DigestMethod xades:Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" xmlns:xades="http://uri.etsi.org/01903/v1.1.1#"/>
        <xades:DigestValue xmlns:xades="http://uri.etsi.org/01903/v1.1.1#">97245346a9b191bfef4b82f0ef018f17efb217ca</xades:DigestValue>
      </tsp:DigestAlgValue>
    </tsp:File>
  - <tsp:Certificate tsp:URI="signedSTC.xml">
    - <tsp:DigestAlgValue Id="HEX(SHA-1(STC file)">
        <xades:DigestMethod xades:Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" xmlns:xades="http://uri.etsi.org/01903/v1.1.1#"/>
        <xades:DigestValue xmlns:xades="http://uri.etsi.org/01903/v1.1.1#">121be6de8fdf54892c010c18f1274516456856ab</xades:DigestValue>
      </tsp:DigestAlgValue>
    </tsp:Certificate>
  - <ds:Signature Id="SigmaSignatureElement" xmlns:xades="http://uri.etsi.org/01903/v1.1.1#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:sta="http://sta" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:gml="http://www.opengis.net/gml"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    - <ds:SignedInfo Id="SignedInfoElement">
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      - <ds:Reference URI="#Message">
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>UMQTbkvo5TqK84eEHic3B1AgTAU=</ds:DigestValue>
        </ds:Reference>
      - <ds:Reference URI="#Certiloc STC">
        - <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>SVP0mg9ucqCZJ4XxllJxyobBDZk=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue> JnC6MVTPvZ0TuAmHg9QqiuGX0WkJnGf+lT2GsY5rYBdFhrlF0zeRcNoPpJQ3zGhq5ZzfVfGf53Y0
        4p18gGXGmkvbL7UYEEA9uIu6DSA25kPH0hq2qgSjJV9/JAbcdCHeY/s1uyc6EEPd70NmCgkFqEEQ vm0xqucFecml5qDvUCY= </ds:SignatureValue>
    - <ds:KeyInfo Id="Certificates_of_Subject">
      - <ds:X509Data>
          <ds:X509Certificate> MIIE2zCCA8OgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBuDELMAkGA1UEBhMCRVMxDzANBgNVBAgT
            Bk1BRFJJRDEpMCcGA1UEChMgVW5pdmVyc2lkYWQgQ2FybG9zIElJSSBkZSBNYWRyaWQxITAfBgNV
            BAsTGERlcGFydGFtZW50byBJbmZvcm1hdGljYTEkMCIGA1UEAxMbQ0EgRGVwYXJ0YW1lbnRvIElu
            Zm9ybWF0aWNhMSQwIgYJKoZIhvcNAQkBFhVDQUluZm9ybWF0aWNhQHVjM20uZXMwHhcNMTIxMDEw
            MTEwOTMwWhcNMTMxMDEwMTEwOTMwWjCBqTELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1BRFJJRDEp
            MCcGA1UEChMgVW5pdmVyc2lkYWQgQ2FybG9zIElJSSBkZSBNYWRyaWQxITAfBgNVBAsTGERlcGFy
            dGFtZW50byBJbmZvcm1hdGljYTEWMBQGA1UEAxMNUmF1bCBNYXJ0aW5lejEjMCEGCSqGSIb3DQEJ
            ARYUcmF1bG1hcnRpbmV6QHVjM20uZXMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKQvYDpL
            GLE5g7BCA0WFPpFQwWmvZVEBrMtPdQDUr0OJn3VziHFNVvWjZHNrXv4+HYlEqsu9MHuO9naH8mgo
            9i9yNWcrLZEoaEfdVSvflUlk00Eh8nhaVQn5JA2Q5E6QCST6Aao4p/c490fwX+AAAt4DeU1QLn0k
            oNwlR+KC9EIvAgMBAAGjggF/MIIBezAMBgNVHRMEBTADAgEAMBEGCWCGSAGG+EIBAQQEAwIEsDAs
```


Ilustración 16 – Contenido del CET, documento M y firma Sigma

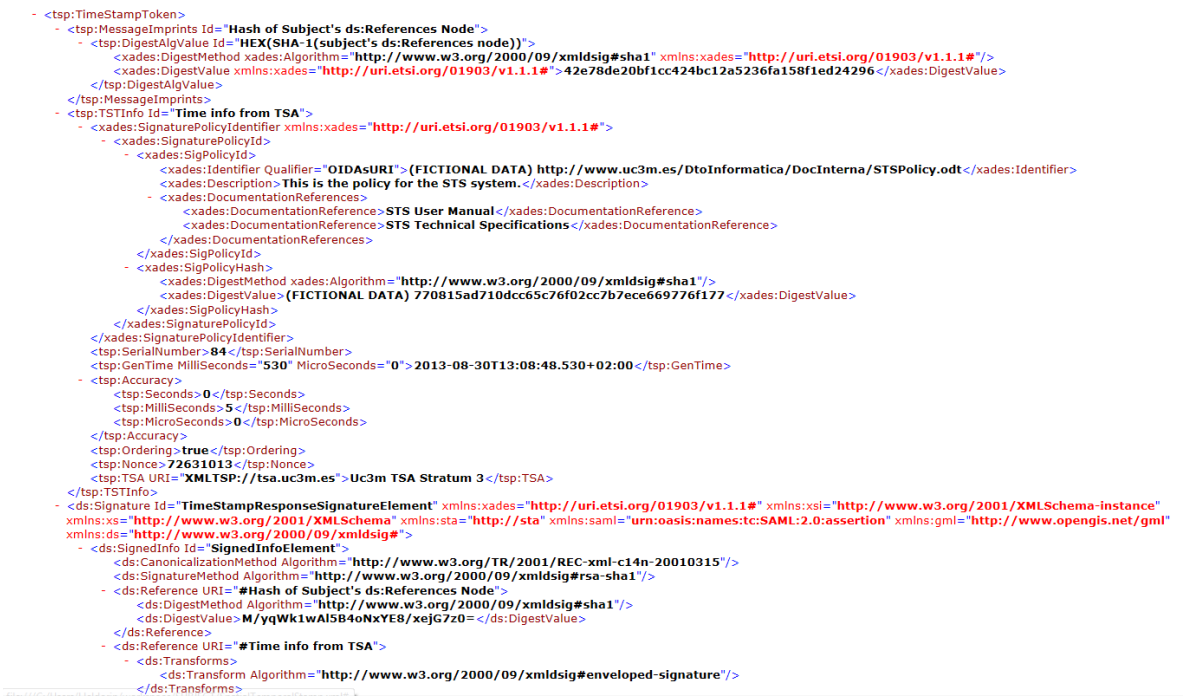


Ilustración 17 - Contenido del sello temporal

No obstante, el sistema desarrollado en [1] tiene un problema a la hora de afrontar el objetivo de este TFG, y es la complejidad de la estructura del código. El módulo cliente depende de unas librerias externas almacenadas en un proyecto paralelo (véase la Ilustración 18 donde se expande la estructura del código de los proyectos STSS y COMMON, necesarios para implementar el SUBJECT), lo que dificulta su migración directa a un dispositivo móvil.

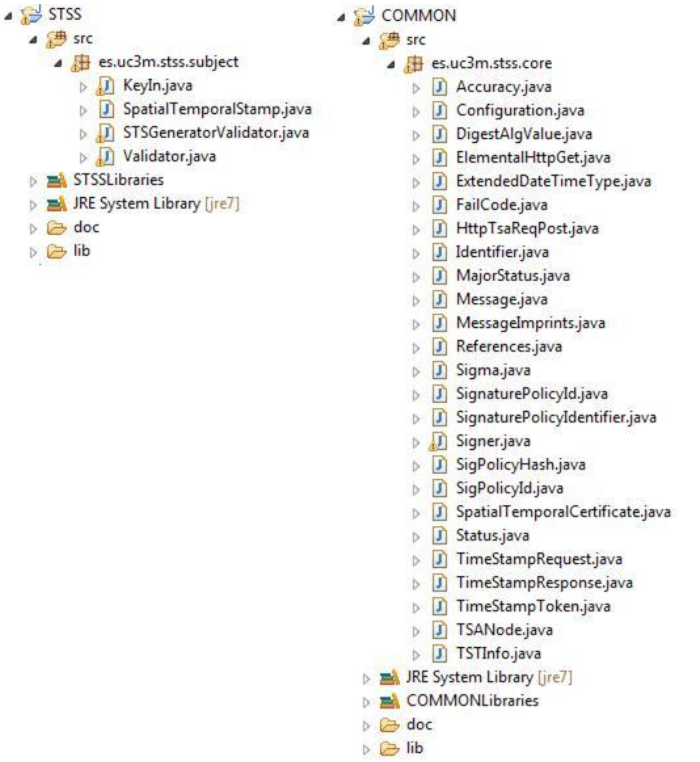


Ilustración 18 - Código de SUBJECT [1]

4. ANÁLISIS DEL SISTEMA

Este capítulo tiene como objetivo analizar los cambios que es necesario hacer en [1] para que el sistema sea compatible con una plataforma Android, así como las soluciones propuestas a los problemas encontrados.

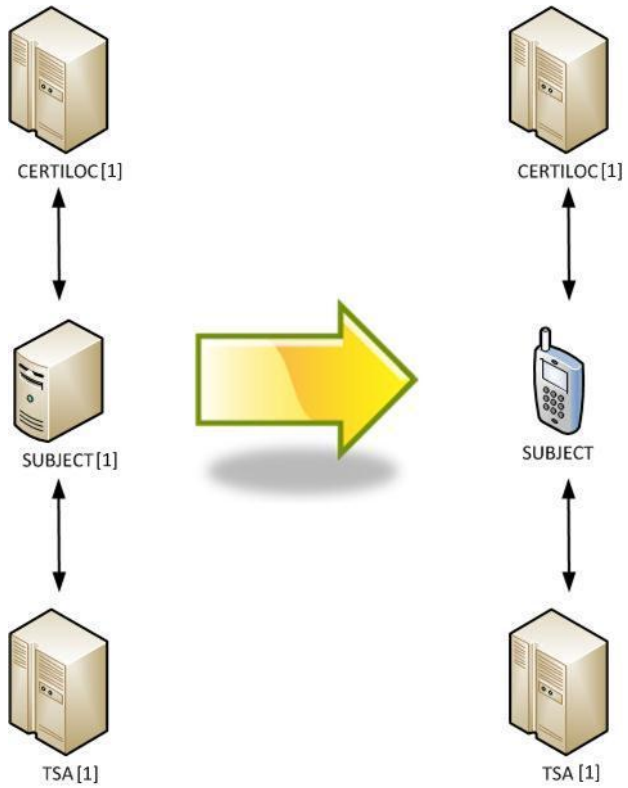


Ilustración 19 - Objetivo del TFG

4.1. Selección del sistema operativo del dispositivo móvil, el lenguaje de programación y la librería de seguridad XML

En el presente proyecto consiste en la adaptación de la entidad SUBJECT del sistema realizado en [1] a un dispositivo móvil. Se decidió que dicho dispositivo deberá de tener **sistema operativo Android** por las siguientes razones:

- Al ser un sistema operativo de código abierto, da mayores facilidades para el desarrollo de aplicaciones que otros sistemas operativos de dispositivos móviles como iOS o Windows Phone.

- Android es el sistema operativo con mayor cuota en el mercado móvil y con una mayor velocidad de crecimiento.
- Al tener como lenguaje de programación de aplicaciones una versión de Java denominada Java Android SDK; ya que el sistema desarrollado en [1] está programado en Java bajo el entorno de desarrollo Eclipse. Por tanto, el lenguaje de programación elegido es **Java Android SDK**.

Sin embargo, Java Android SDK no soporta todas las librerías disponibles de Java. Dado que se necesita contar con la funcionalidad de generar y validar firmas digitales será necesario modificar la entidad SUBJECT para que sea compatible con este lenguaje.

Los paquetes necesarios para la generación de firmas digitales bajo el estándar XMLDSig son *javax.xml.crypto, javax.xml.crypto.dsig, javax.xml.crypto.dsig.keyinfo, javax.xml.crypto.dsig.spec, javax.xml.crypto.dom, javax.xml.crypto.dsig.dom*. Estos paquetes pueden encontrarse, principalmente, en las librerías Apache Santuario [9] o Java WSPD.

En principio, la información con la que se contaba al inicio del proyecto indicaba que la librería Apache Santuario [9] podría proporcionar una solución para realizar firmas digitales XML en un dispositivo Android. Así que ésta es la librería seleccionada como librería de seguridad XML.

4.2. Aproximación en dos fases: Simplificación del SUBJECT y migración a Android SDK

Como se ha indicado anteriormente, el sistema [1] está desarrollado en lenguaje de programación Java utilizando el entorno de desarrollo Eclipse. La entidad SUBJECT se compone de varios ficheros .class de Java mediante los cuales se realizan los procesos de conexión HTTP, generación de firmas XML de documentos y validación de dichas firmas. Estos ficheros están repartidos en el propio proyecto STSS, que representa la entidad denominada SUBJECT en este TFG, y en un grupo de librerías adyacentes

llamado COMMON, que contiene .class comunes a las tres entidades (SUBJECT, CERTILOC y TSA).

Sin embargo, varias de las librerías utilizadas para dichos procesos (por ejemplo, joda-time o xercesImpl) no son compatibles con Java Android SDK, por lo que se necesita modificar los procesos que las usan para que puedan ser desplegados en un sistema móvil Android. Este es el principal objetivo de este Trabajo Fin de Grado.

Para alcanzar el objetivo, se decide afrontar el proyecto en dos fases tal y como se refleja en el planteamiento inicial del capítulo 2. Gestión del Proyecto.

- Fase 1A: En primer lugar, se va a realizar una **simplificación del código del SUBJECT [1]** de forma que el proceso de firma posea una estructura de software más sencilla y ligera; ya que las plataformas móviles son más ligeras y poseen menos capacidades que los ordenadores convencionales. Esta simplificación del código generará una nueva entidad SUBJECT que realizará las mismas funciones que las realizadas en [1], pero de un modo más simple, sin depender de los .class del proyecto COMMON. Esta entidad SUBJECT se denominará SUBJECT 1A, dado que es el principal resultado de la fase 1A. Nótese que, a pesar de considerarse las mismas funcionalidades que en [1], se ha añadido una funcionalidad más. La generación de firmas digitales seguirá siendo igual que en [1], mediante la utilización de una clave privada (y su certificado de clave pública asociado) que deberá estar alojada en el propio SUBJECT.

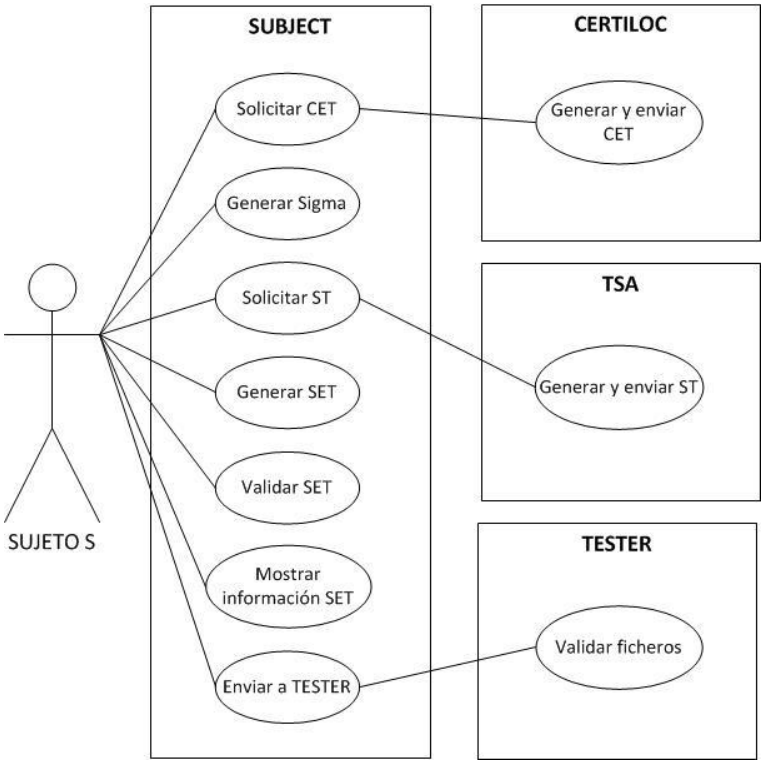


Ilustración 20 - Casos de uso de Fase 1A.

- Fase 2A: Posteriormente, se realizará la **migración de las librerías no compatibles con Java Android SDK**, para que el proyecto pueda ser desplegado en dispositivos Android. De esta manera, se dispondrá de dos entidades cliente: una desplegada en un ordenador de mesa (SUBJECT 1A) y otra en un dispositivo móvil (que se denominará correspondientemente SUBJECT 2A); pudiendo ambas interactuar de manera autónoma con las entidades CERTILOC [1] y TSA [1].

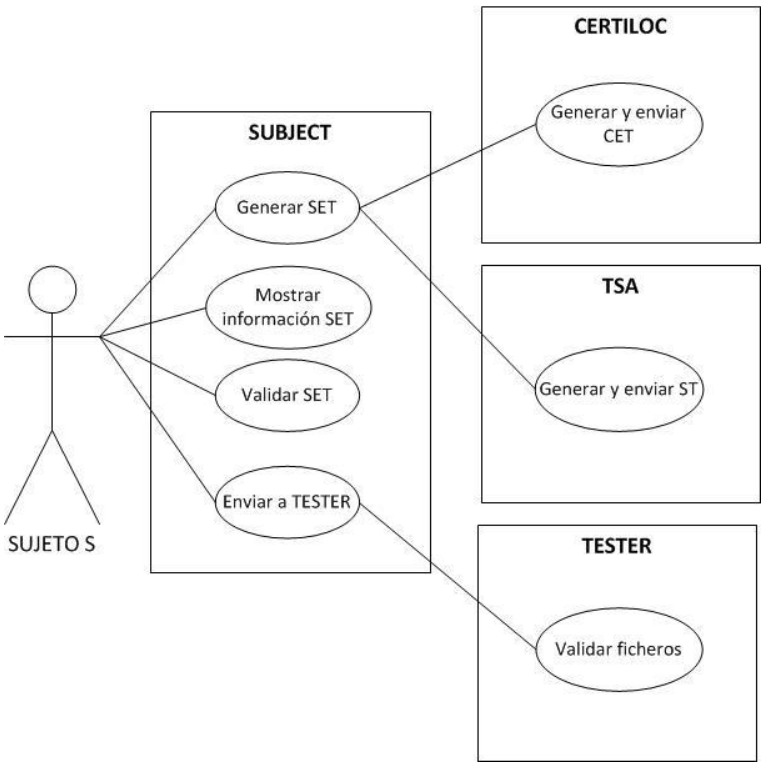


Ilustración 21 - Casos de uso de fase 2A.

Por tanto, la arquitectura a alto nivel del sistema quedaría compuesta de tres entidades cliente, dos desplegadas en ordenadores (SUBJECT [1] y SUBJECT 1A) y otra desplegada en dispositivo móvil (SUBJECT 2A), que tendrían comunicación con las entidades CERTILOC y TSA para poder generar sellos espacio-temporales (ver ilustración 22).

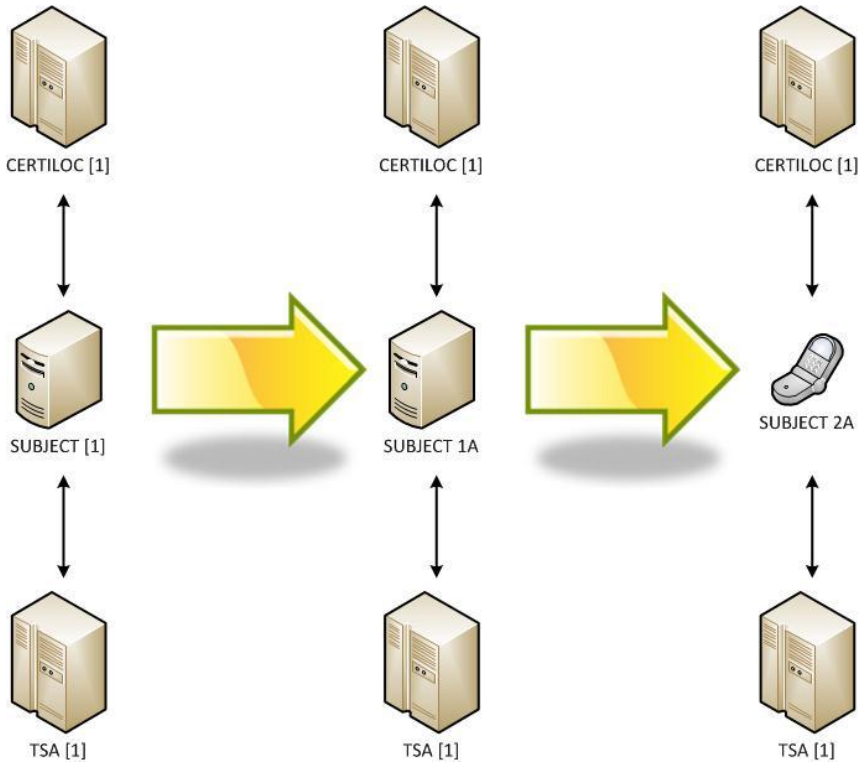


Ilustración 22 – Arquitectura parcial (conexiones con CERTILOC y TSA) según las dos fases consideradas.

Paralelamente a la arquitectura presentada, se debe añadir una nueva entidad que tendrá conexión con el SUBJECT.

Dicha entidad se llamará TESTER y hará las funciones del destinatario final que recibirá el documento M, el CET y el SET (ver ilustración 23). Esta entidad permite satisfacer un requisito no contemplado en [1], que es la simulación de un receptor final del SET. Este receptor tendrá que comprobar que todos los datos incluidos en el CET y el SET son correctos para aceptar la firma generada por el sujeto.

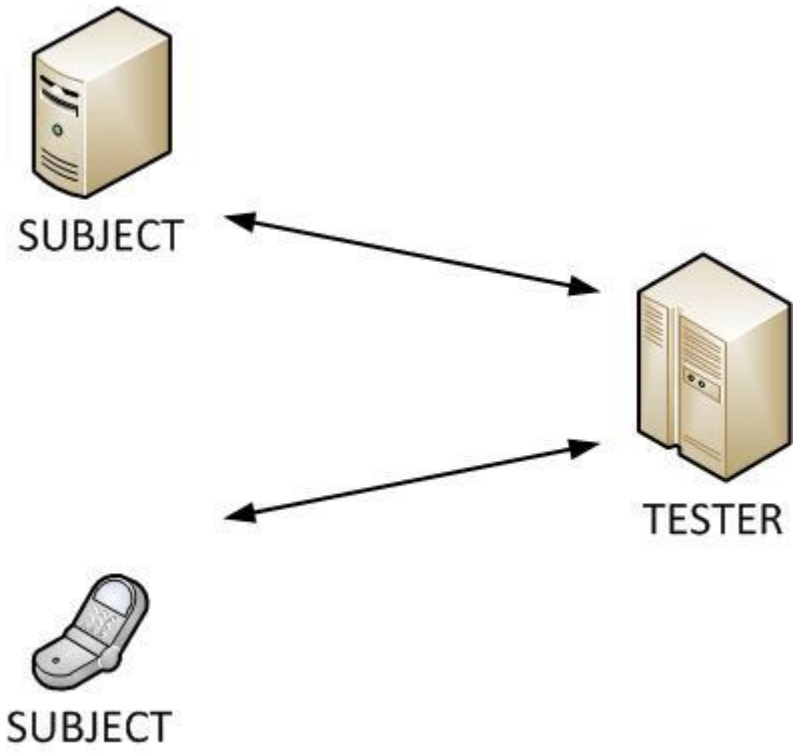


Ilustración 23 - Arquitectura parcial del sistema de (conexión con TESTER).

Puesto que Android posee sus propios protocolos de conexión HTTP, el punto en común entre el nuevo SUBJECT 1A resultado de la fase 1A y su migración a Java Android SDK (SUBJECT 2A) debe ser el código para la generación y validación de firmas XML. Como se ha mencionado en el apartado anterior. Se decide utilizar la misma librería que utiliza [1], Apache Santuario [14] versión 1.4.6, ya que resulta compatible con los sistemas Android. Esta librería ofrece la posibilidad de generar y validar firmas digitales XML siguiendo el estándar XMLDSig a través de varios de sus paquetes.

Sin embargo, el proceso de generación y validación de firmas en Android tiene un problema, ya que Java Android SDK no es capaz de implementar el paquete XMLSignature de la librería Apache Santuario [14], utilizada para el tratamiento de firmas XML. Para encontrar la razón se debe de buscar en [16], donde se indica lo siguiente: "*The usual code for XML signing that works on regular Java does not work on Android because of differences in padding initialization*". Obviamente, esta información no se conoció hasta que ya se estaba abordando la fase 2A, y solo se llegó hasta ella

tratando de encontrar las razones por las que no estaba teniendo éxito la migración del SUBJECT 1A al SUBJECT 2A.

Para solucionar esta incapacidad de Android, existen dos soluciones posibles: crear un sistema propio de generación/validación de firmas XML desde el dispositivo sin el soporte de una librería o utilizar un servicio digital de generación/validación de firmas (DSS).

Se estudiaron ambas opciones y se llegó a la conclusión de que la primera opción, crear un sistema de tratamiento de firmas XML desde el dispositivo, era inviable para mantener la estructura de firmas que utiliza el proyecto CERTILOC y que la complejidad de realizar dicho software excedía el alcance propuesto del Trabajo Fin de Grado. Por lo tanto, se decidió utilizar un servidor DSS para el tratamiento de firmas, que es la razón que motiva la revisión de la arquitectura del sistema, que se expone en el siguiente apartado. Por último, a consecuencia de las circunstancias y las decisiones tomadas, se desea remarcar que no ha sido posible implementar el SUBJECT 2A que estaba previsto como resultado de la fase 2A.

4.3. Revisión de la arquitectura del sistema: adición de la entidad DSS.

La necesidad de un servicio DSS supone una reorganización de la arquitectura desarrollada hasta ahora para incluir un servidor que nos proporcione dicho servicio. Se deber modificar el SUBJECT desarrollado en el planteamiento inicial para añadir un sistema de generación y validación de firmas mediante el uso de DSS. De este modo, la arquitectura resultante contará con tres servicios: CERTILOC, que emitirá los certificados espacio-temporales; TSA, que emitirá sellos temporales; y DSS, que generará y validará firmas.

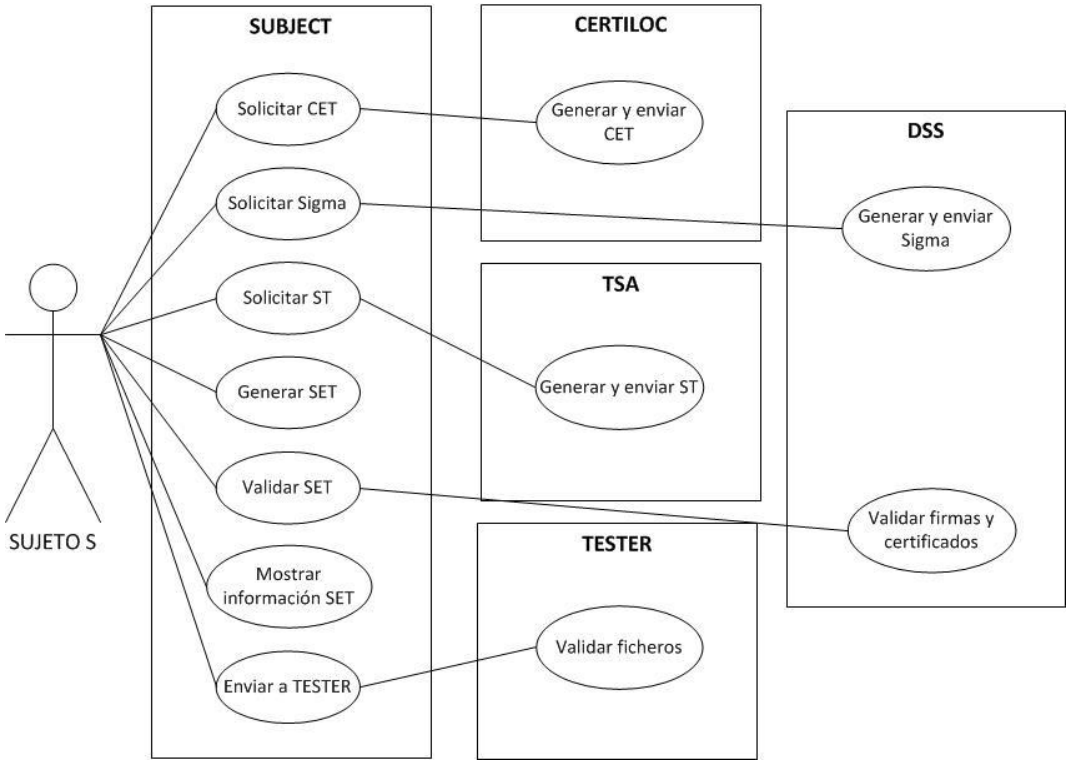


Ilustración 24 - Casos de uso de fase 1B.

El desarrollo del sistema se vuelve a plantear en dos fases que equivalen a las fases 1A y 2A pero considerando la nueva arquitectura:

- Fase 1B: a partir del código desarrollado en SUBJECT 1A, se implementará una nueva entidad que **utilizará el servicio DSS** para la generación y validación de firmas digitales. Esta nueva entidad se la denominará SUBJECT 1B.
- Fase 2B: nuevamente, se realizará la **migración de las librerías no compatibles con Java Android SDK**, para que el proyecto pueda ser desplegado en dispositivos Android. Dicha migración dará como resultado una entidad cliente ejecutable en sistemas Android, que se denominará SUBJECT 2B.

Se busca que el sistema resultado de la fase 1A sea compatible con el desarrollo de las fases 1B y 2B. Por tanto, al finalizar el proyecto, existirán tres entidades SUBJECT simultáneas (véase ilustración 25 y tabla 22):

- SUBJECT 1A: que genere y valide sus propias firmas
- SUBJECT 1B: que utilice el DSS para el tratamiento de firmas

- SUBJECT 2B: que será la implementación en Android de SUBJECT 1B.

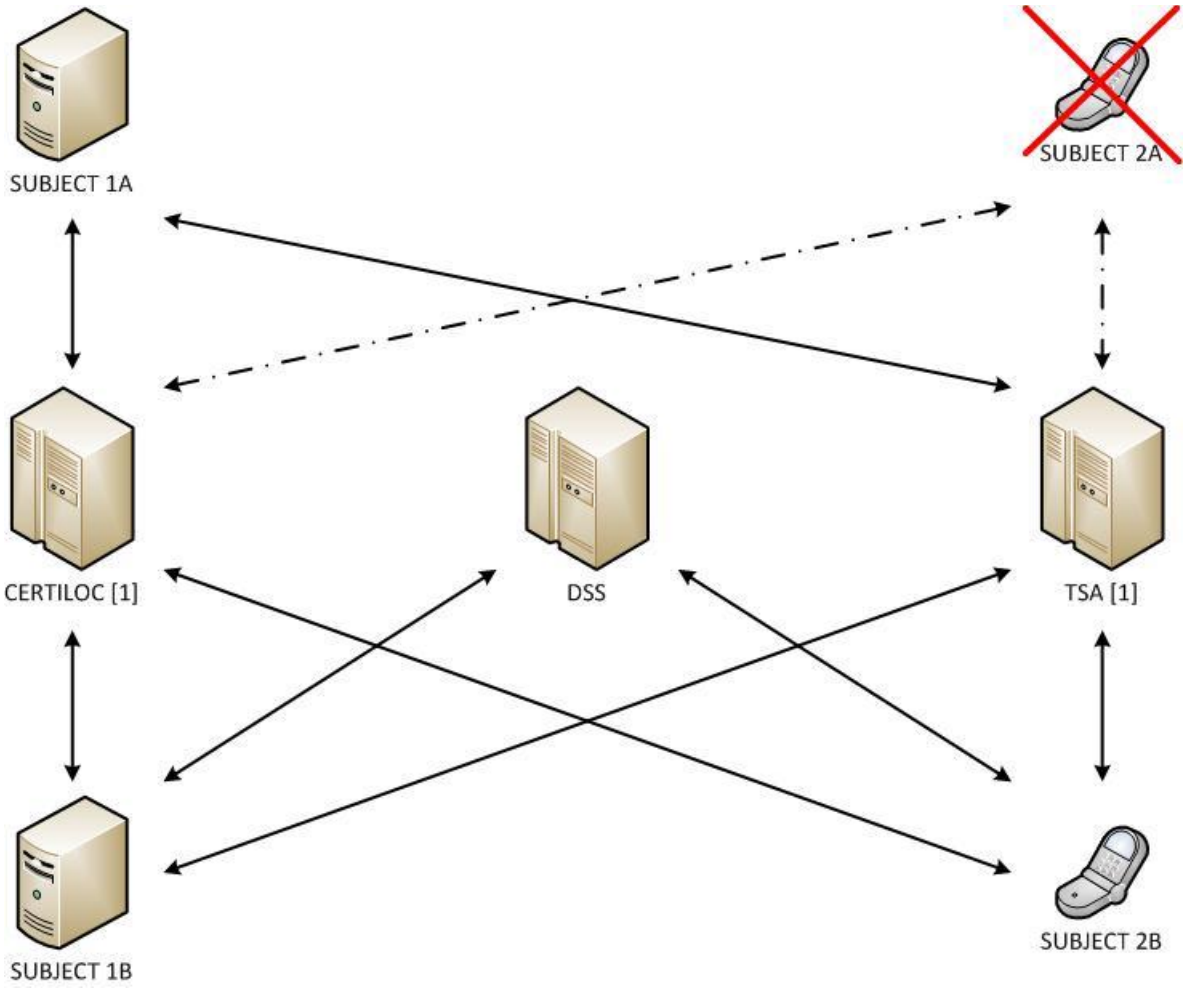


Ilustración 25 - Arquitectura revisada.

	SUBJECT 1A	SUBJECT 2A	SUBJECT 1B	SUBJECT 2B
Método de generación de firmas digitales.	Autónomo	No genera firmas digitales.	Mediante DSS	Mediante DSS
Lenguaje de programación.	Java estándar	Java Android SDK	Java estándar	Java Android SDK

Tabla 22 - Comparativa de las entidades SUBJECT generadas

Para la codificación del DSS se utilizará la estructura de conexión HTTP de entidades ya implementadas (CERTILOC y TSA) para la conexión entre un SUBJECT y el servidor DSS. Dicho servidor tendrá dos funcionalidades principales:

- **Generar firmas digitales**; para lo que se necesitará información sobre un fichero y un certificado. Dicha información será el nombre del fichero, ya que el nombre del certificado será un estándar, y el resumen criptográfico de ambos documentos calculados con el algoritmo Sha-1 (para preservar la privacidad de los documentos). Esta funcionalidad devolverá un fichero XML (Sigma) que contendrá la firma realizada e información sobre el fichero y el certificado. Para que el servidor DSS sea capaz de generar estas firmas digitales en nombre del SUBJECT, se utilizará la misma clave privada (y su certificado de clave pública asociado) usada en SUBJECT 1A.

- **Validación de firmas digitales**; para lo que necesitará el fichero y el certificado sobre el que se generaron las firmas, y las propias firmas digitales. En el ámbito de este proyecto, dado que todas las firmas existentes en el sello espacio-temporal están enlazadas, se decide que el cliente envíe directamente el sello espacio-temporal (SpatialTemporalStamp) que las contiene. El DSS sólo validará firmas y certificados, omitiendo otras comprobaciones como las fechas o los hash. Esta funcionalidad retornará el resultado de validar las firmas y certificados de los documentos.

Sin embargo, al establecer estas funcionalidades aparece el problema de cómo hacer saber al DSS que fichero se le está enviando. Por ello, se hace uso de los códigos HTTP para que el servicio sepa que fichero o petición está recibiendo. El diseño del método de conexión con el DSS, así como el envío y tratamiento de estos códigos, será detallado en el capítulo 5.5 Módulo DSS.

Una vez se ha desarrollado por completo el DSS, se modifica el SUBJECT 1A generado en la planificación inicial para quitarle la generación de Sigma y la validación de las firmas del sello espacio-temporal; e incluirle la conexión y envío de ficheros al DSS y la validación de la información que no procesa el DSS (las fechas de los certificados y los hash almacenados). El resultado de este proceso, el SUBJECT 1B, será el que,

posteriormente, se migrará a una plataforma Android obteniendo el objetivo final de este TFG, que se ha denominado SUBJECT 2B.

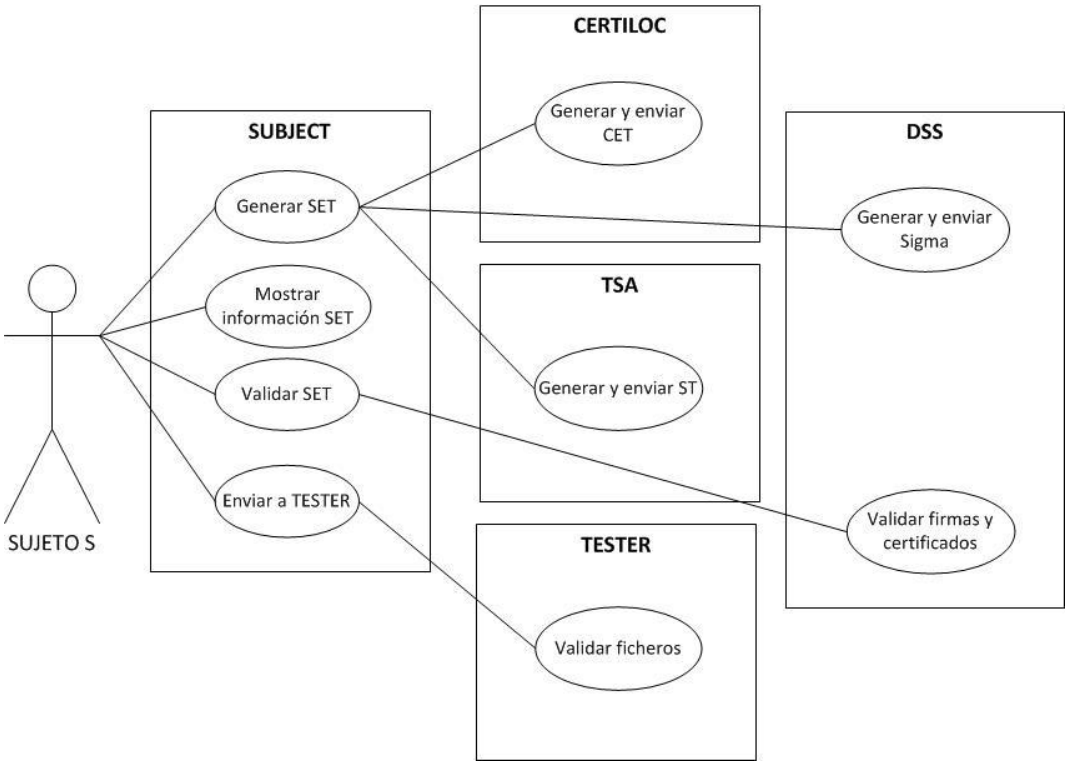


Ilustración 26 - Casos de uso de fase 2B.

4.4. Plan de pruebas

Una vez analizado el sistema y planteada la arquitectura definitiva, se necesita un plan de pruebas concreto para evaluar correctamente el buen funcionamiento de la aplicación.

Ya que el objetivo final del TFG es desplegar la aplicación en un dispositivo móvil, se determina la realización de las pruebas únicamente en SUBJECT 2B, ya que se considera la entidad objetivo del TFG, desestimando realizar pruebas en SUBJECT 1A, SUBJECT 1B, CERTILOC y TSA.

No obstante, ya que para la inclusión en la arquitectura de los módulos DSS y TESTER fue necesario hacer diversas pruebas, se mostrarán las pruebas realizadas con ellos desde SUBJECT 1B. Para cada prueba sigue un modelo en el que se define:

- ID: identificador único para cada prueba que seguirá el estándar PRxxx donde xxx es una secuencia numérica que comienza en 001.
- Título: título descriptivo sobre qué consiste la prueba.
- Descripción: pasos necesarios para realizar la prueba.
- Resultado esperado: sucesos que tienen que ocurrir para dar por superada la prueba.

A continuación se muestran las pruebas que se realizarán sobre el sistema. El resultado de las pruebas puede verse en el capítulo 6. Pruebas.

ID	PR001
Título	Conexión básica exitosa del cliente con CERTILOC.
Descripción	Seleccionar un archivo. Pulsar en *Generate SpatialTemporalStamp*.
Resultado esperado	CERTILOC responde a las peticiones.

Tabla 23 - PR001: Conexión básica exitosa del cliente con CERTILOC.

ID	PR002
Título	Solicitud correcta de generación de CET a CERTILOC.
Descripción	Seleccionar un archivo. Pulsar en *Generate SpatialTemporalStamp*.
Resultado esperado	CERTILOC envía el CET.

Tabla 24 - PR002: Solicitud correcta de generación de CET a CERTILOC.

ID	PR003
Título	Recepción correcta del CET desde CERTILOC.
Descripción	Seleccionar un archivo. Pulsar en *Generate SpatialTemporalStamp*.
Resultado esperado	El cliente almacena el CET. Mensaje correcto de generación del SET.

Tabla 25 - PR003: Recepción correcta del CET desde CERTILOC.

ID	PR004
Título	Conexión básica exitosa del cliente con DSS.
Descripción	Seleccionar un archivo. Pulsar en *Generate SpatialTemporalStamp*.
Resultado esperado	DSS responde a las peticiones.

Tabla 26 - PR004: Conexión básica exitosa del cliente con DSS.

ID	PR005
Título	Solicitud correcta de generación de firmas al DSS.
Descripción	Seleccionar un archivo. Pulsar en *Generate SpatialTemporalStamp*.
Resultado esperado	DSS envía Sigma.

Tabla 27 - PR005: Solicitud correcta de generación de firmas al DSS.

ID	PR006
Título	Recepción correcta de Sigma desde el DSS.
Descripción	Seleccionar un archivo. Pulsar en *Generate SpatialTemporalStamp*.
Resultado esperado	El cliente almacena Sigma. Mensaje correcto de generación del SET.

Tabla 28 - PR006: Recepción correcta de Sigma desde el DSS.

ID	PR007
Título	Envío correcto de ficheros al DSS.
Descripción	Seleccionar un archivo. Pulsar en *Validate SpatialTemporalStamp*.
Resultado esperado	DSS responde OK (200).

Tabla 29 - PR007: Envío correcto de ficheros al DSS.

ID	PR008
Título	Conexión básica exitosa del cliente con TSA.
Descripción	Seleccionar un archivo. Pulsar en *Generate SpatialTemporalStamp*.
Resultado esperado	TSA responde a las peticiones.

Tabla 30 - PR008: Conexión básica exitosa del cliente con TSA.

ID	PR009
Título	Envío correcto de la petición de ST a TSA.
Descripción	Seleccionar un archivo. Pulsar en *Generate SpatialTemporalStamp*.
Resultado esperado	TSA envía el ST (*TimeStampResponse*).

Tabla 31 - PR009: Envío correcto de la petición de ST a TSA.

ID	PR010
Título	Recepción correcta de ST desde TSA.
Descripción	Seleccionar un archivo. Pulsar en *Generate SpatialTemporalStamp*.
Resultado esperado	El cliente almacena el ST. Mensaje de generación del SET correcto.

Tabla 32 - PR010: Recepción correcta de ST desde TSA.

ID	PR011
Título	Conexión básica exitosa del cliente con TESTER.
Descripción	Seleccionar un archivo. Pulsar en *Send to TesterService*.
Resultado esperado	TESTER responde a las peticiones.

Tabla 33 - PR011: Conexión básica exitosa del cliente con TESTER.

ID	PR012
Título	Envío correcto de ficheros (mensaje, CET y SET) a TESTER.
Descripción	Seleccionar un archivo. Pulsar en *Send to TesterService*.
Resultado esperado	TESTER responde OK (200) a cada envío.

Tabla 34 - PR012: Envío correcto de ficheros (mensaje, CET y SET) a TESTER.

ID	PR013
Título	Generación correcta de la petición de ST (*TimeStampRequest*) por parte del cliente.
Descripción	Seleccionar un archivo. Pulsar en *Generate SpatialTemporalStamp*.
Resultado esperado	TSA envía el ST (*TimeStampResponse*). El cliente almacena el ST. Mensaje de generación del SET correcto.

Tabla 35 - PR013: Generación correcta de la petición de ST (TimeStampRequest) por parte del cliente.

ID	PR014
Título	Generación correcta del SET (*SpatialTemporalStamp*) por parte del cliente.
Descripción	Seleccionar un archivo. Pulsar en *Generate SpatialTemporalStamp*.
Resultado esperado	Mensaje de generación del SET correcto.

Tabla 36 - PR014: Generación correcta del SET (SpatialTemporalStamp) por parte del cliente.

ID	PR015
Título	Generación correcta de firmas por parte del DSS.
Descripción	Seleccionar un archivo. Pulsar en *Generate SpatialTemporalStamp*. Esperar a que finalice el proceso. Pulsar en *Validate SpatialTemporalStamp*.
Resultado esperado	Mensaje de generación del SET correcto. Mensaje de validación correcta de firmas y certificados por parte del DSS.

Tabla 37 - PR015: Generación correcta de firmas por parte del DSS.

ID	PR016
Título	Validación correcta de firmas y certificados por parte del DSS.
Descripción	Seleccionar un archivo. Pulsar en *Validate SpatialTemporalStamp*.
Resultado esperado	Mensaje de validación correcta de firmas y certificados por parte del DSS.

Tabla 38 - PR016: Validación correcta de firmas y certificados por parte del DSS.

ID	PR017
Título	Validación correcta de los resúmenes criptográficos del SET por parte del cliente.
Descripción	Seleccionar un archivo. Pulsar en *Validate SpatialTemporalStamp*.
Resultado esperado	Mensaje de validación correcta de resúmenes criptográficos.

Tabla 39 - PR017: Validación correcta de los resúmenes criptográficos del SET por parte del cliente.

ID	PR018
Título	Validación correcta de las fechas del SET por parte del cliente.
Descripción	Seleccionar un archivo. Pulsar en *Validate SpatialTemporalStamp*.
Resultado esperado	Mensaje de validación correcta de fechas.

Tabla 40 - PR018: Validación correcta de las fechas del SET por parte del cliente.

ID	PR019
Título	Validación completa del SET por parte del TESTER.
Descripción	Seleccionar un archivo. Pulsar en *Send to TesterService*.
Resultado esperado	Mensaje de aceptación desde TESTER.

Tabla 41 - PR019: Validación completa del SET por parte del TESTER.

ID	PR020
Título	Visualización correcta de los detalles del SET por parte del cliente (CERTILOC APP).
Descripción	Seleccionar un archivo. Pulsar en *Generate SpatialTemporalStamp*. Esperar a que finalice el proceso. Pulsar en *Show SpatialTemporalStamp Info*.
Resultado esperado	Visualización sin errores de los detalles del SET.

Tabla 42 - PR020: Visualización correcta de los detalles del SET por parte del cliente (CERTILOC APP).

ID	PR021
Título	Visualización correcta de la interpretación del SET por parte del cliente (CERTILOC MAPS).
Descripción	Seleccionar un archivo. Pulsar en *Generate SpatialTemporalStamp*. Esperar a que finalice el proceso. Ejecutar la aplicación CERTILOC MAPS.
Resultado esperado	Visualización sin errores de la interpretación del SET.

Tabla 43 - PR021: Visualización correcta de la interpretación del SET por parte del cliente (CERTILOC MAPS).

ID	PR022
Título	Mensaje de error al intentar generar o validar el SET o al intentar enviar a TESTER y no haber seleccionado un fichero.
Descripción	No haber seleccionado un fichero. Pulsar en *Generate SpatialTemporalStamp*, *Validate SpatialTemporalStamp*, o *Show SpatialTemporalStamp Info*.
Resultado esperado	Mensaje de que no se ha seleccionado un fichero. La aplicación no se bloquea.

Tabla 44 - PR022: Mensaje de error al intentar generar o validar el SET o al intentar enviar a TESTER y no haber seleccionado un fichero.

ID	PR023
Título	Mensaje de error sin bloqueo de aplicación al intentar visualizar la interpretación del SET con fecha del CET posterior a la fecha del SET (CERTILOC MAPS).
Descripción	Tener un CET con fecha posterior a la del SET. Ejecutar CERTILOC MAPS.
Resultado esperado	Mensaje de que las fechas no son correctas. La aplicación no se bloquea.

Tabla 45 - PR023: Mensaje de error sin bloqueo de aplicación al intentar visualizar la interpretación del SET con fecha del CET posterior a la fecha del SET (CERTILOC MAPS).

4.5. Análisis socio-económico.

El sistema desarrollado en este TFG o en los Proyectos Fin de Carrera anteriores no tendría ningún sentido si no pudieran ser utilizados de algún modo en la sociedad actual y pudiera recuperarse la inversión inicial.

La primera pregunta que surge es ¿cómo y/o dónde puede aplicarse el sistema desarrollado en este TFG? Obviamente, el principal escenario dónde poder ser utilizado es aquel que necesite certificar que un sujeto se encontraba en cierto lugar en cierto momento (a través de la firma de un documento) o directamente que se necesite probar que dicho documento se firmó en cierta área geográfica y momento temporal. A día de hoy, esto puede ser necesario en los siguientes casos:

- Administración Pública, para la firma de documentos públicos u otras actividades (atestados, etc.).
- Empresas privadas de ámbitos concretos, como podrían ser las compañías de seguros o en el ámbito del comercio internacional (firma de contratos, acceso a servicios, etc. por las diferentes coberturas ofrecidas por las legislaciones y regulaciones de los países en caso de litigios).
- Particulares que deseen certificar documentos, por ejemplo firma de contratos o compras por internet, o en aplicaciones concretas como pueden ser los servicios de apuestas electrónicas (por las diferentes legislaciones existentes en la actualidad en cada país o estado).

En vista de estas tres opciones, aparecen dos posibles mercados de negocio para la aplicación. Por un lado, la venta completa del sistema a la Administración Pública o a alguna empresa particular, a los que se les podría ofrecer por el presupuesto calculado en el capítulo 2.4 Análisis Económico.

Por otro, se podría vender la aplicación a particulares como una APP en Google Play. Para ello, se estimaría la venta de la aplicación a un precio de 2€ después de observar el precio de aplicaciones similares (Firma Digital FNMT, qPDF Notes). A una media de

300 ventas al mes de la aplicación, se reembolsaría la inversión inicial junto con los beneficios en cuatro años.

No obstante, lo mencionado anteriormente solo afectaría a la entidad cliente (SUBJECT) de la aplicación. Para el resto de entidades que proporcionan los servicios de confianza en los que se basa la construcción y validación del SET (CERTILOC, TSA y DSS) habría que considerar varios asuntos antes de proceder a su comercialización o puesta en servicio.

Al ser servicios que se podrían clasificar como de provisión de servicios certificación electrónica [10], no es posible hacer un despliegue descuidado de estos. Antes de proceder a la venta de estas entidades del sistema, sería necesario, primero, dotar al código actual de las suficientes garantías de seguridad, en particular, en relación con el servicio de DSS (en el que habría que abordar al menos los asuntos de seguridad que han quedado fuera del alcance de este proyecto). En segundo lugar, sería necesario satisfacer los requisitos técnicos que impone la legislación vigente a este tipo de servicios (se asume la entidad responsable de su provisión satisfará los requisitos administrativos). Todo ello encarecería el precio de venta del sistema, dado que se debería imputar al menos los costes sobrevenidos por la modificación del código actual derivados de satisfacer los requisitos técnicos.

Otra opción, sería sustituir estas entidades por servicios gratuitos equivalentes, de los que podría beneficiarse el público particular. Lamentablemente, solo existen en la actualidad servicios gratuitos de sellado temporal (podrían sustituir a la TSA) pero no emiten sellos temporales en XML, sino según el RFC 3161 [27]. No existen servicios que ofrezcan de forma gratuita certificados espacio-temporales (CERTILOC) o firmas digitales delegadas (DSS).

4.6. Análisis de la legislación relacionada

En este apartado se analiza brevemente la legislación relacionada con el TFG. El sistema desarrollado en este TFG está afectado por la legislación existente principalmente en dos aspectos. El primero de ellos es la protección de los datos de carácter personal, entre los que se puede encuadrar la localización de un dispositivo fácilmente asociable a un individuo en un momento dado. El segundo de ellos sería el posible reconocimiento legal de la firma generada por el sujeto, y objeto principal del sello espacio-temporal, así como la legitimidad del servicio de sellado espacio-temporal en términos regulatorios.

Cuando la información espacio-temporal está asociada a una persona física, se entra en el ámbito de la privacidad de datos personales, determinado por la Ley 15/99, Orgánica de protección de datos de carácter personal, 1999, que establece que el afectado debe poder decidir para qué y cómo se procesan dichos datos.

En la ley 59/2003 [10] se exponen las bases reguladoras para la utilización de la firma electrónica, su eficacia jurídica y su utilidad en los servicios de certificación.

Gracias a esta ley se podría hacer un uso real de los certificados electrónicos y los servicios de certificación contemplados en el sistema, ya que en el artículo 5 estipula que "*la prestación de servicios de certificación no está sujeta a autorización previa y se realizará en régimen de libre competencia*".

No obstante, en el artículo 17 se indica explícitamente la necesidad de tratar los datos personales que precisen el uso de estos servicios de certificación bajo "*lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en sus normas de desarrollo*". Es por ello que los datos requeridos para el correcto funcionamiento del servicio de generación del servicio de sellado espacio-temporal deberían ser única y exclusivamente los necesarios para la realización de los correspondientes certificados y la firma digital de documentos, todos ellos bajo las bases impuestas en la Ley General de Comunicaciones 32/2003 [11].

Si se desease que la firma generada por el sujeto tuviese eficacia jurídica, habría de contemplarse lo establecido en [10]. Se puede resaltar que actualmente existen algunos servicios públicos que hacen uso de dicha firma electrónica con eficacia jurídica en el ámbito del sector público, por ejemplo, en el ámbito de la factura electrónica [12] o en interacciones con la Agencia Tributaria.

Por último, el sistema desarrollado en el TFG está bastante relacionado con las recientes regulaciones promulgadas para el establecimiento y puesta en marcha de servicios telemáticos en el ámbito de varios organismos públicos (Agencia Tributaria, Ministerio de Economía y Hacienda y Ministerio de Industria y Turismo). Por ejemplo, el artículo 45 de la Ley 30/1992 [13] dispone que las Administraciones Públicas, en especial el Ministerio de Economía y Hacienda, impulsarán la aplicación de técnicas telemáticas para el desarrollo de sus actividades y proporcionarán dicho servicio a los ciudadanos. Este tipo de servicios suelen contar con "*un registro telemático para la recepción y tramitación de los escritos, solicitudes y comunicaciones que se remitan y expidan por vía telemática mediante firma electrónica avanzada en el ámbito de los procedimientos y actuaciones incluidos en el anexo I de la presente Orden*". Salvando las distancias, se podría decir que estos registros son similares al servicio de sellado espacio-temporal desarrollado en este TFG.

5. DISEÑO E IMPLEMENTACIÓN

Una vez que se ha especificado qué es lo que debe realizar cada entidad desarrollada en el capítulo anterior, en este capítulo se expone el diseño de bajo nivel del conjunto del sistema software.

La fase de diseño, habitualmente, se trabaja en dos fases: la organización general de los componentes del software o "diseño arquitectónico"; y cómo se estructura internamente cada uno de los componentes o "diseño detallado". En este Proyecto, el diseño arquitectónico viene definido desde [1], pues simplemente se debe realizar la migración de uno de sus componentes software. En la fase de análisis se ha añadido un componente adicional a esa arquitectura establecida pero sin modificarla. De alguna manera, el diseño arquitectónico preexistente formaba parte de la caracterización del problema a analizar.

Por ello, en este capítulo se describe cada entidad del sistema planteado en la fase de Análisis. Se describirán las entidades en el orden de creación o modificación de los mismos en base a la planificación inicial y la revisión de la misma.

Así, inicialmente se expondrán las modificaciones realizadas en los módulos ya existentes (CERTILOC y TSA); para después abordar los nuevos módulos desarrollados en la planificación inicial y sus respectivas revisiones.

Para diferenciar entre los distintos clientes del sistema se utilizará la fase correspondiente de la planificación del proyecto.

5.1. Módulo CERTILOC

Ya que en el objetivo del presente proyecto no formaba parte una reestructuración de este módulo, no se ha modificado su arquitectura ni su diseño tanto en la planificación inicial como en el diseño final.

No obstante, debido a las librerías de conexión HTTP que utiliza Android, al implementar SUBJECT 2B fue necesario incluir una línea de código adicional en el módulo que elimine los símbolos "/" existentes en la petición HTTP. Esto se debe a que al procesar la petición desde el dispositivo móvil, el módulo cogía el símbolo "/" (ver cuadro rojo en ilustración 27) como parte del nombre del fichero y no podía almacenarlo, ya que Windows no permite guardar nombres de ficheros que contengan ese símbolo.

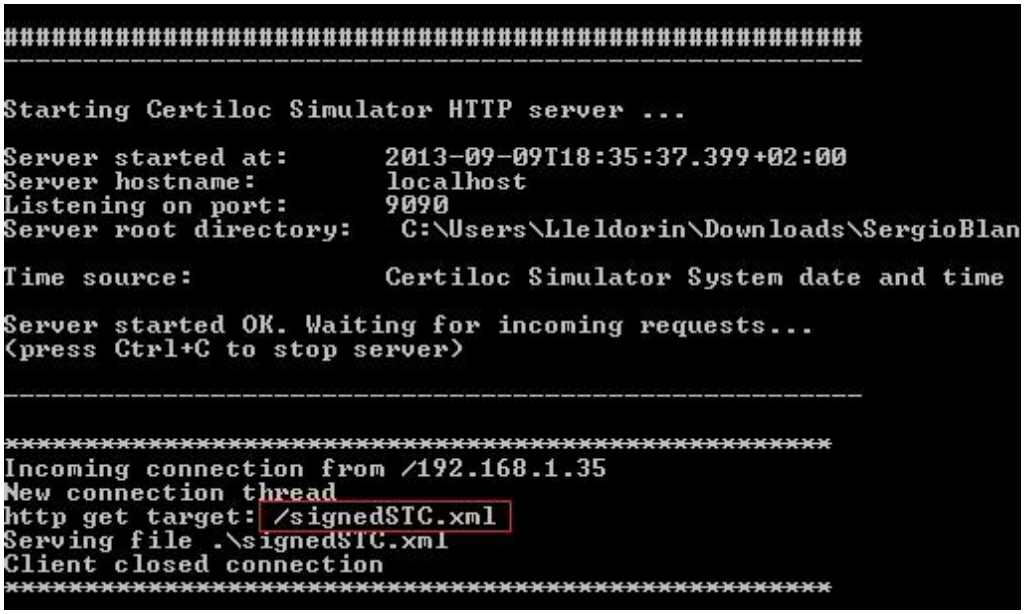


Ilustración 27 - Módulo CERTILOC procesando erróneamente la petición

Al no poder almacenar el certificado generado, el módulo CERTILOC enviaba al cliente el último certificado almacenado, por lo que la fecha y localización del mismo no sería adecuada para el sello que se pretende generar. En la tabla 46 se puede ver un comparativo resumen entre como procesa las peticiones CERTILOC dependiendo desde donde se le envíe:

	Ordenador	Android
Petición enviada	http://certiloc:9090/signedSTC.xml	
Petición procesada	signedSTC.xml	/signedSTC.xml
Nombre CET	signedSTC.xml	/signedSTC.xml
Envío CET correcto	Sí	No

Tabla 46 - Diferencia de procesado de petición en CERTILOC

En la ilustración 28 se puede observar cómo procesa las peticiones después de introducir el cambio en el código.

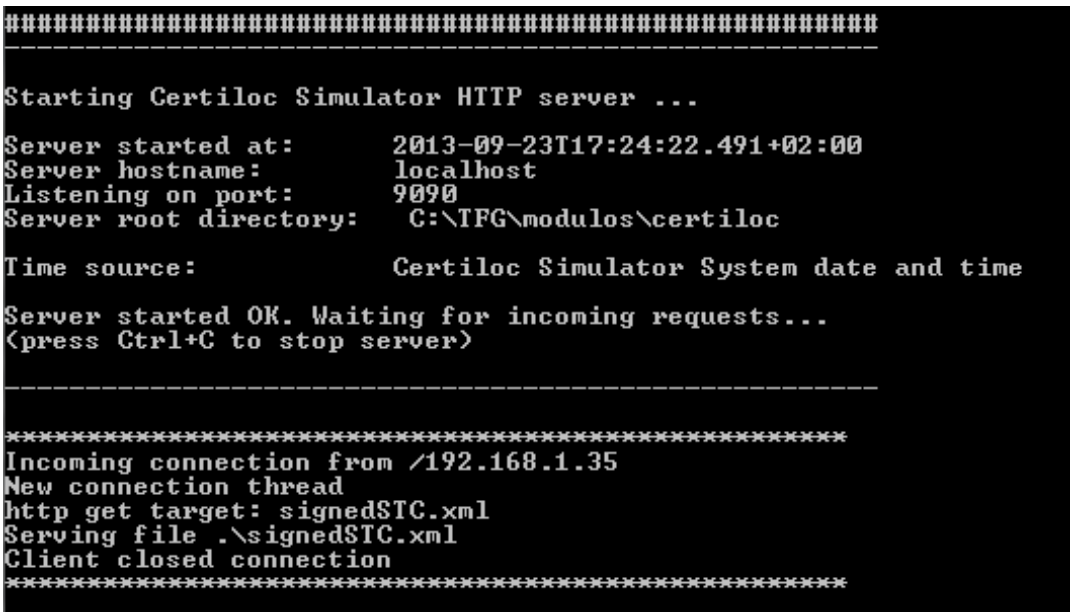


Ilustración 28 - Módulo CERTILOC procesando correctamente la petición.

5.2. Módulo TSA

Ya que en el objetivo del presente proyecto no formaba parte una reestructuración de este módulo, no se ha modificado su arquitectura ni su diseño tanto en la planificación inicial como en el diseño final.

En este módulo no surgió el problema del símbolo / al intentar conectarlo con un dispositivo Android, ya que la propia petición del *TimeStamp* ya incluye dicho símbolo y lo trata debidamente.

5.3. Módulo SUBJECT 1A

5.3.1. Diseño

En el módulo cliente del sistema presentado en [1] se mostraba al usuario una interfaz por línea de comando mediante la cual pueda ejecutar las distintas opciones posibles, dependiendo de si se ejecutaba como usuario normal o usuario administrador. Ya que lo que se realiza en este punto es una simplificación de dicho módulo, se utilizará el diseño de usuario administrador de [1] para crear la interfaz (ver tabla 47).

Opción	Función
1. Get Spatial Temporal Certificate	Realiza la petición del certificado espacio-temporal y lo almacena si es bien recibido.
2. Generate Sigma	Genera Sigma mediante el certificado y el fichero que se introduzca por teclado.
3. Request Timestamp	Genera TimeStampRequest, solicita TimeStampResponse y lo almacena si es bien recibido.
4. Create Spatial Temporal Stamp	Crea el fichero SpatialTemporalStamp mediante Sigma y TimeStampResponse si existen en el directorio raíz.
5. Execute 1,2,3 and 4	Ejecuta los pasos del 1 al 4 con las iteraciones necesarias con el usuario
6. Validate Spatial Temporal Stamp	Realiza la comprobación de firmas, certificados, hashes y fechas en el certificado y sello espacio-temporal
7. Clean up generated files	Borra todos los ficheros del proceso de creación del sello espacio-temporal.
8. Exit	Cierra la aplicación

Tabla 47 - Opciones de SUBJECT 1A

5.3.2. Implementación

A nivel externo, el proceso de creación del sello espacio-temporal no ha cambiado. Sin embargo, se han creado unas nuevas clases para el proceso de creación de los ficheros XML diferentes al SUBJECT generado en [1].

La generación de los documentos XML, con sus respectivas firmas y certificados, se realiza con la versión 1.4.6 de la librería Apache Santuario [14] por lo que no causará problemas al interactuar con los módulos CERTILOC y TSA. Para generar y validar firmas digitales, se usará la clave privada y el certificado de clave pública que se utilizó en [1], un almacén de certificados de tipo JKS situado en el directorio raíz del proyecto, con dichas credenciales almacenada directamente en el código del proyecto.

Los tres módulos desarrollados en [1] utilizaban las clases de un proyecto aparte que contenía clases comunes utilizadas por los tres módulos. Sin embargo, se necesita ser independientes de dicho proyecto para aligerar el peso de la aplicación y poder implementarla en un dispositivo móvil.

La estructura del módulo dentro del workspace se puede ver en la ilustración 29.

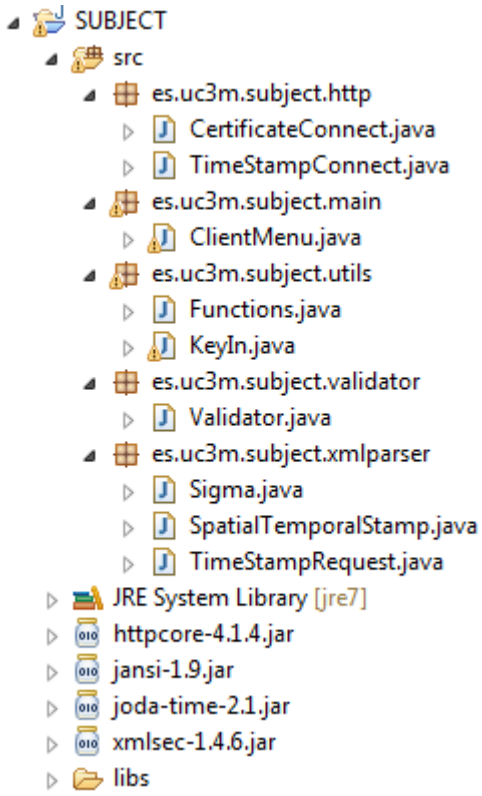


Ilustración 29 - Estructura workspace SUBJECT 1ª

El proceso de creación del Sello Espacio-Temporal no se ha modificado, por lo que se mantiene igual que en el cliente [1], como se puede ver en la ilustración 30.

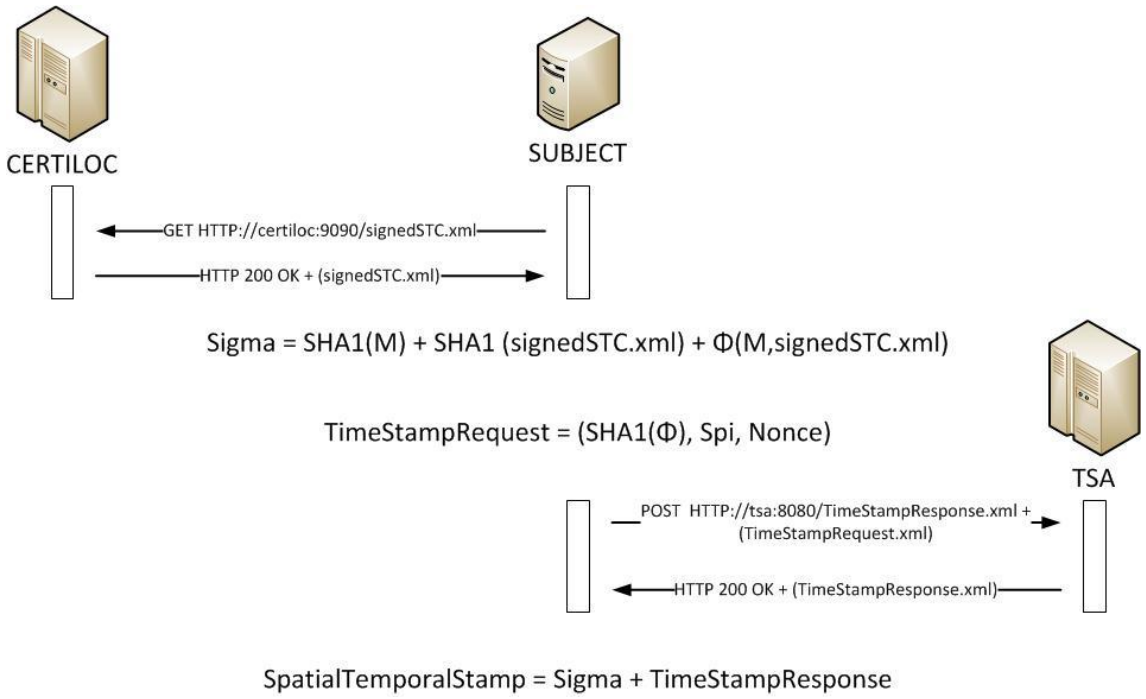


Ilustración 30 - Proceso de creado del sello espacio-temporal en 1A

Diagrama de Clases

En la ilustración 31 se puede ver el diagrama de clases del proyecto. En la tabla 48 se pueden ver con detalle dichas clases.

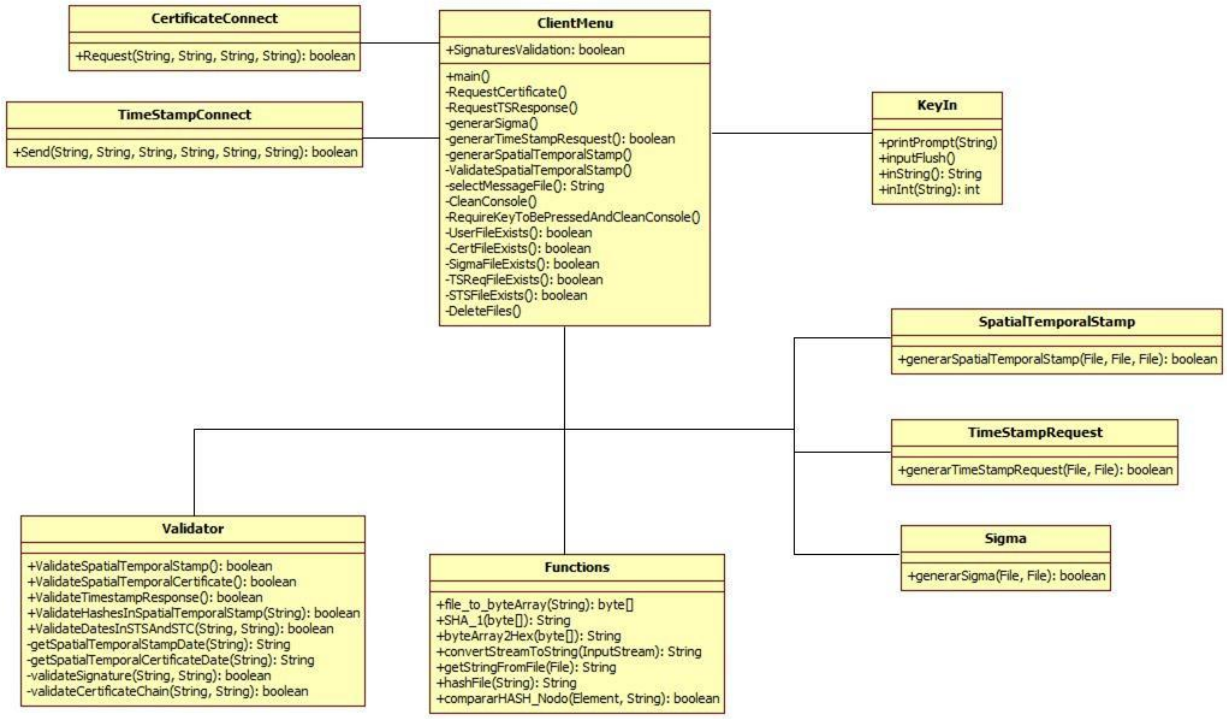


Ilustración 31 - Diagrama de clases de SUBJECT 1A

CLASE	FUNCIÓN
ClientMenu	Mostrar la interfaz de control del programa, manejar las opciones del menú e interaccionar con el usuario.
KeyIn	Ayudar al usuario a interaccionar con la línea de comando.
Functions	Almacenar funciones comunes para varias clases diferentes.
CertificateConnect	Crear la conexión con el módulo CERTILOC, enviar la petición correspondiente y recibir y almacenar el certificado.
TimeStampConnect	Crear la conexión con el módulo TSA, enviar la petición correspondiente y recibir y almacenar el sello temporal.
Sigma	Generar Sigma.xml
TimeStampRequest	Generar TimeStampRequest.xml
SpatialTemporalStamp	Generar SpatialTemporalStamp.xml
Validator	Validar las firmas, certificados, hashes y fechas del sello espacio-temporal y los certificados.

Tabla 48 - Clases de SUBJECT 1A

Dependencia de librerías externas

En la tabla 49 se pueden ver las librerías del proyecto.

Nombre	Origen	Empaquetado	Función
Apache HttpComponents 4.1.4	http://hc.apache.org/	httpcore-4.1.4.jar	Crear las conexiones con CERTILOC, TSA y enviar/recibir ficheros. Con ambas entidades.
Jansi 1.9	http://jansi.fusesource.org/	jansi-1.9.jar	Manejar la salida por pantalla en línea de comando.
Joda Time 2.1	http://joda-time.sourceforge.net/	joda-time-2.1.jar	Calcular diferencias entre las fechas del certificado y el sello temporal.
Apache Santuario 1.4.6	http://santuario.apache.org/	xmlsec-1.4.6.jar	Manipular instancias de la clase XMLSignature poder generar y verificar firmas

Tabla 49 - Librerías de SUBJECT 1A

5.4. Módulo SUBJECT 2A

Este módulo consiste en la implementación en Java Android SDK del módulo SUBJECT 1A. Sin embargo, como se dijo anteriormente, la librería XMLSignature necesaria para generar y validar firmas no puede ser implementada por este lenguaje de programación debido a diferencias en el mecanismo de inicialización del *padding* con respecto al lenguaje Java clásico.

No se llegó a implementar ningún código en este módulo más allá de las pruebas realizadas para generar firmas digitales XMLDSig. Por ello, los detalles del diseño e implementación de la aplicación Android serán explicados en el apartado Módulo SUBJECT 2B.

5.5. Módulo DSS

5.5.1. Diseño

Este módulo debe servir como generador y validador de firmas digitales XML en nombre de un sujeto. En un diseño completo del sistema, el cliente y el servidor DSS previamente deben establecer un contrato y generar un certificado a nombre del sujeto,

que será almacenado en el directorio raíz del servidor junto con la clave privada asociada para ser utilizado para tratar las firmas. En este TFG no se incluye dicha funcionalidad, por no formar parte de los objetivos del trabajo, por lo que se presupone la realización de dicho contrato con anterioridad al uso de la aplicación.

El módulo DSS tiene dos funcionalidades: generar firmas digitales sobre un fichero y un certificado espacio-temporal y validar las firmas de un sello espacio-temporal y los ficheros que lo componen. Cualquier otro tipo de generación o validación será externo a este servicio.

Para mantener la privacidad del sujeto a la hora de generar firmas digitales, el DSS solo recibirá los resúmenes del fichero y el certificado espacio-temporal. No obstante, para validar las firmas digitales necesitará los documentos al completo.

Por lo tanto, las distintas entidades cliente que se conecten al DSS deben de poder enviarle tanto resúmenes como ficheros. Además, aunque el nombre de los distintos sellos y certificados son comunes en todos los módulos, el nombre del fichero sobre el cual se desea generar el sello espacio-temporal es desconocido para el DSS, por lo que también será necesario su envío.

Para la comunicación cliente-DSS se ha decidido utilizar códigos de estado HTTP no utilizados normalmente en las conexiones estándar (ver tabla 50). Se comprobaron los códigos utilizados para las peticiones estándar [17] y se eligieron los siguientes códigos, no utilizados para dichas peticiones.

Códigos de solicitudes:	
250	Solicitud de generación de Sigma.
252	Solicitud de validación de sello espacio-temporal
Códigos de envío de información al DSS	
260	Envío del fichero.
262	Envío del certificado.
264	Envío del sello espacio-temporal.
266	Envío del hash del fichero.
268	Envío del hash del certificado.
Códigos de respuesta del DSS al realizar la validación	
254	Las firmas y certificados correctos
255	Las firmas y certificados erróneos.
550	Se ha producido un error en el DSS al realizar la validación

Tabla 50 - Códigos de conexión con el DSS

Un cliente se conecta al servicio DSS a través del puerto 7070 de la máquina de hospedaje del servidor mediante una conexión de tipo POST. Dependiendo del tipo de información que le envíe, solo realizará la petición (solo al enviar hashes o peticiones de generación/validación de firmas) o además anexará ficheros. Sea como fuere, la estructura general de la petición será la siguiente:

$$POST\ HTTP://dss{:}7070/code{:}opt1{:}opt2$$

Dónde:

- Code: código de solicitud que envía el cliente.
- Opt1: campo opcional donde se anexa el nombre del fichero (al enviar el fichero o su hash) o el hash del certificado.
- Opt2: campo adicional solo utilizable cuando se envía el hash del fichero para anexar el valor del mismo.

Es importante recalcar en la utilización del símbolo ':' para separar el código de la información anexada, pues es el símbolo que utiliza el servidor para distinguir entre la

información que recibe. Además, aunque las distintas medidas de seguridad posibles de incluir en este tipo de conexiones no han sido estudiadas por salirse de los objetivos del TFG, se ha decidido que la conexión sea de tipo POST ya que se envían datos en claro.

Para tener una mejor claridad de cómo son las peticiones, en la tabla 51 se muestran todos los tipos de peticiones con su estructura particular:

Petición del Cliente	Sintaxis petición POST
Generación de Sigma.	http://dss:7070/250
Validación de sello espacio-temporal	http://dss:7070/252
Envío del fichero.	http://dss:7070/260:FileName + (FILE)
Envío del certificado.	http://dss:7070/262 + (CERT)
Envío del sello espacio-temporal.	http://dss:7070/264 + (STAMP)
Envío del hash del fichero.	http://dss:7070/266:FileName:FileHash
Envío del hash del certificado.	http://dss:7070/268:CertHash

Tabla 51 - Sintaxis de peticiones al DSS

En general, el DSS responderá a estas peticiones con un código 200 si ha ido todo bien o con un código 404 si el código enviado no es correcto o los ficheros no pudieron ser almacenados. Las únicas excepciones son:

- Código 250: el servidor devolverá el fichero Sigma.xml anexado a la respuesta.
- Código 252: el servidor devolverá uno de estos tres códigos:
  - 254 si todas las firmas y certificados son válidos.
  - 255 si alguna de las firmas o certificados no son válidos.
  - 550 si se produce algún error en el proceso de validación.

El funcionamiento del servicio DSS será similar al de los módulos CERTILOC y TSA.: una vez se ponga en ejecución el servicio, éste se mantendrá a la escucha de las peticiones que pueda recibir. El servicio no está configurado para atender

simultáneamente a varios clientes (de forma similar a CERTILOC y TSA), por lo que se deberán de realizar peticiones de distintos clientes de una en una.

En la ilustración 32 se puede ver la interfaz del servidor.

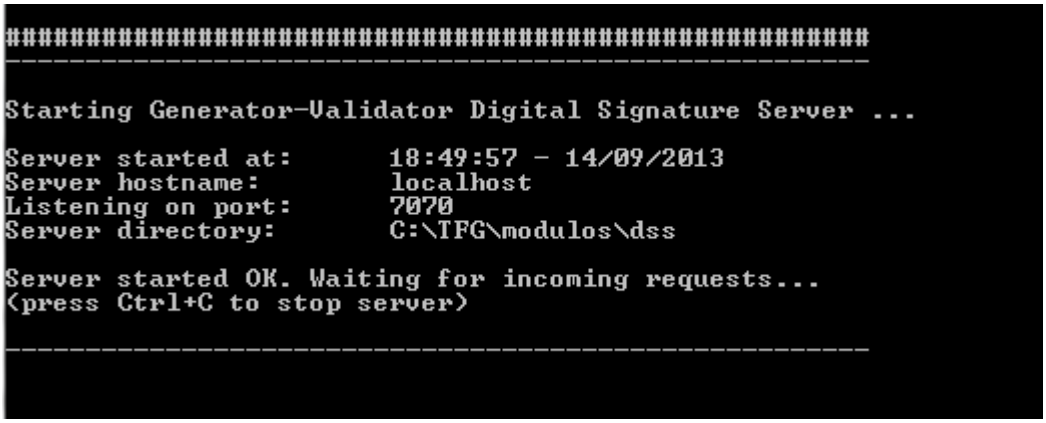


Ilustración 32 - Interfaz del servicio DSS

A continuación se muestran dos diagramas con el proceso de solicitud de generación de firmas (ver ilustración 33) y el proceso de solicitud de validación de firmas (ver ilustración 34).

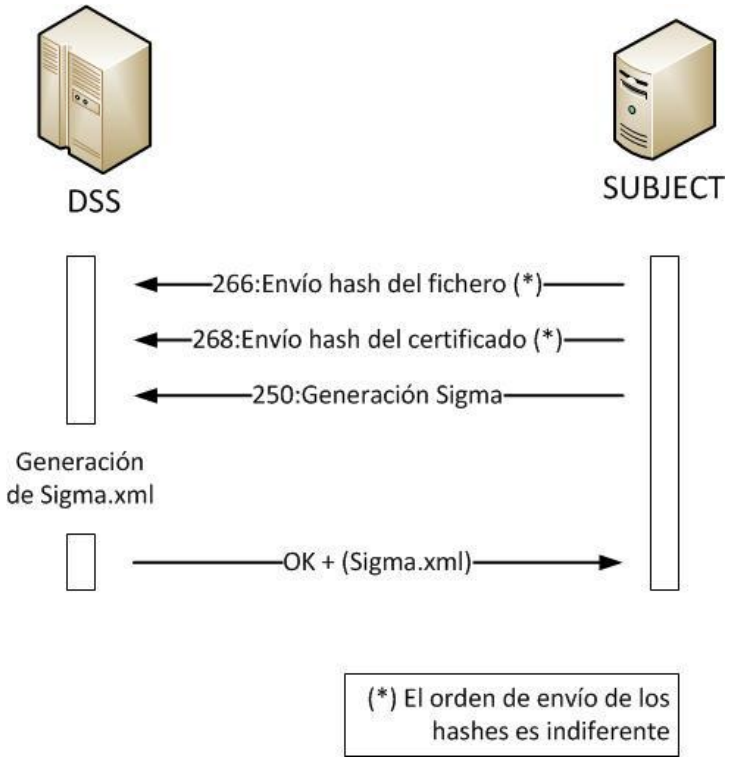


Ilustración 33 - Proceso de generación de firma digital mediante DSS

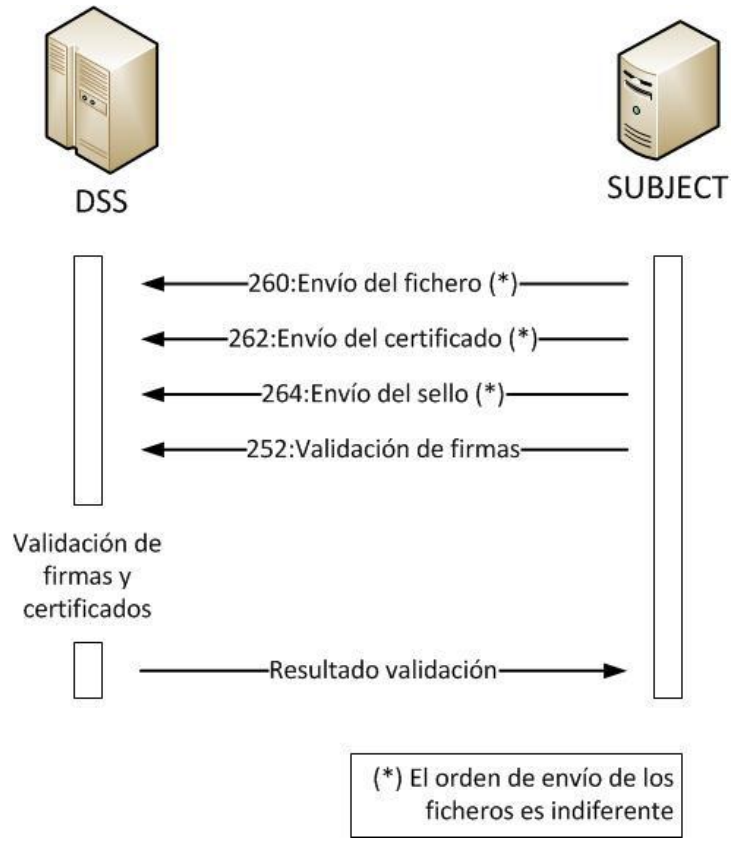


Ilustración 34 - Proceso de validación de firmas digitales mediante DSS

5.5.2. Implementación

Al realizar el diseño del servicio DSS, se decidió que la validación de firmas y certificados fuera más completa que la diseñada previamente en SUBJECT 1A. Para ello, se enlazó el proyecto del servicio DSS con las librerías almacenadas en el proyecto COMMON de [1] para así poder utilizar el sistema de validación de SUBJECT [1]. La estructura del módulo dentro del workspace se puede ver en la ilustración 35

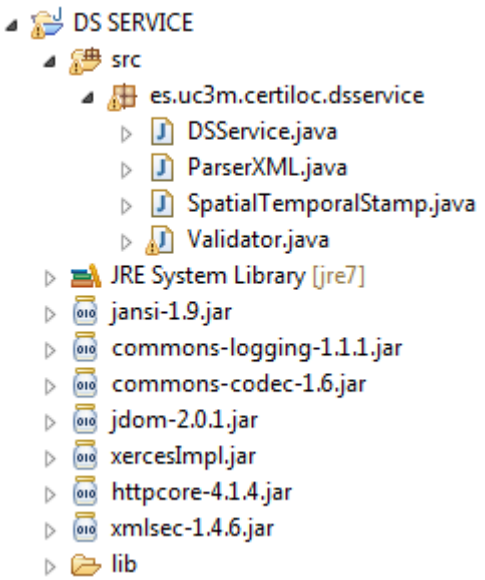


Ilustración 35 - Workspace de DSS

Sin embargo, para la generación de firmas digitales se utilizó el código generado en SUBJECT 1A para darle utilidad al sistema generado previamente. El certificado utilizado será el mismo que en SUBJECT 1A,

almacenado en la carpeta raíz del proyecto. Así mismo, dichas credenciales estarán almacenadas en el código del proyecto.

Diagrama de Clases

En la ilustración 36 se puede ver el diagrama de clases del proyecto. En la tabla 52 se pueden ver con detalle dichas clases.

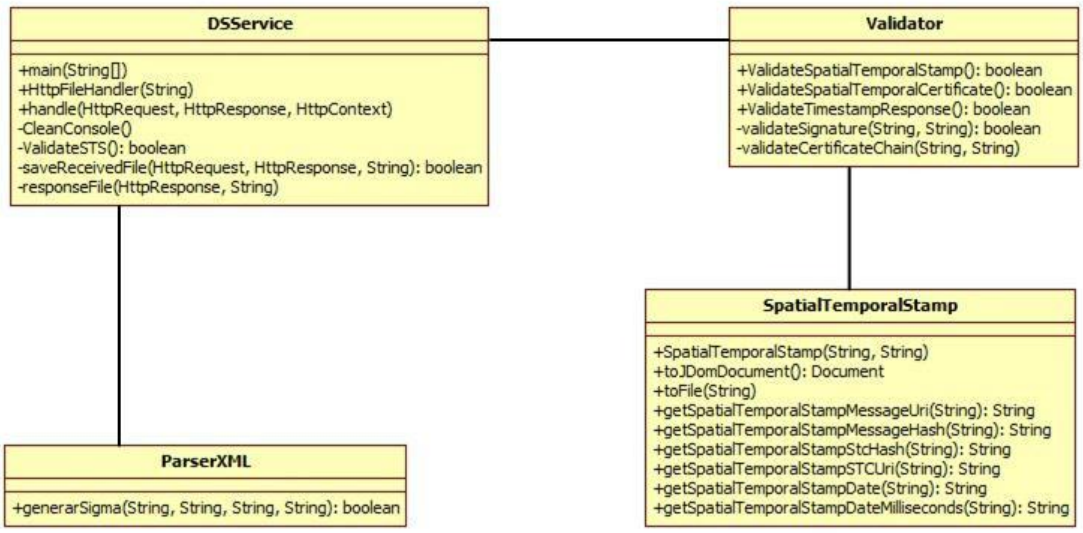


Ilustración 36 - Diagrama de clases de DSS

CLASE	FUNCIÓN
DSService	Mostrar la interfaz del programa, mantenerse a la espera de peticiones http y tramitar dichas peticiones.
ParserXML	Generar Sigma.xml.
Validator	Validar las firmas y certificados del sello espacio-temporal.
SpatialTemporalStamp	Moverse a través del sello espacio-temporal para obtener los datos de las firmas y los certificados.

Tabla 52 - Clases de DSS

Dependencia de librerías externas

En la tabla 53 se pueden ver las librerías del proyecto.

Nombre	Origen	Empaquetado	Función
Apache HttpComponents 4.1.4	http://hc.apache.org/	httpcore-4.1.4.jar	Crear las conexiones con CERTILOC, TSA y enviar/recibir ficheros. Con ambas entidades.
Jansi 1.9	http://jansi.fusesource.org/	jansi-1.9.jar	Manejar la salida por pantalla en línea de comando.
JDOM 2.0.1	http://www.jdom.org/	jdom-2.0.1.jar	Permitir el manejo de documentos XML conforme al modelo de objetos de documento (DOM).
Apache Santuario 1.4.6	http://santuario.apache.org/	xmlsec-1.4.6.jar	Manipular instancias de la clase XMLSignature poder generar y verificar firmas
Xerces	http://www.jdom.org/	xercesImpl.jar	Librería necesaria para el funcionamiento de Jdom y otras invocaciones desde código donde se usa el DOM clásico.
Apache Commons Codec 1.6	http://commons.apache.org/codec/	commons-codec-1.6.jar	Permitir transformar un resumen en formato array de bytes a hexadecimal
Apache Commons Loggin	http://commons.apache.org/proper/commons-logging/	commons-loggin-1.1.1.jar	Sirve para realizar un log (diario) desde un programa en Java con las herramientas de Apache.

Tabla 53 - Librerías de DSS

5.6. Módulo SUBJECT 1B

5.6.1. Diseño

Este módulo es el resultado de modificar SUBJECT 1A para que la generación y validación de firmas digitales resulte operativa mediante el DSS e incluir la conexión con el servicio TESTER.

La interfaz de la aplicación será la misma, pero se añadirá una opción más para enviar los ficheros a TESTER (ver tabla 54).

Opción	Función
1. Get Spatial Temporal Certificate	Realiza la petición del certificado espacio-temporal y lo almacena si es bien recibido.
2. Generate Sigma	Genera Sigma mediante el certificado y el fichero que se introduzca por teclado.

3. Request Timestamp	Genera TimeStampRequest, solicita TimeStampResponse y lo almacena si es bien recibido.
4. Create Spatial Temporal Stamp	Crea el fichero SpatialTemporalStamp mediante Sigma y TimeStampResponse si existen en el directorio raíz.
5. Execute 1,2,3 and 4	Ejecuta los pasos del 1 al 4 con las iteraciones necesarias con el usuario
6. Validate Spatial Temporal Stamp	Realiza la comprobación de firmas, certificados, hashes y fechas en el certificado y sello espacio-temporal
7. Send files to Tester Server	Envía el fichero, el certificado y el sello espacio-temporal a TESTER para que los acepte.
8. Clean up generated files	Borra todos los ficheros del proceso de creación del sello espacio-temporal.
9. Exit	Cierra la aplicación

Tabla 54 - Opciones de SUBJECT 1B

5.6.2. Implementación

Ahora el proceso de generación del sello espacio-temporal es diferente a como se generaba en [1], ya que es necesaria realizar una conexión con el DSS en el proceso.

Esto supone añadir las clases necesarias a la aplicación para realizar las conexiones pertinentes. A diferencia de SUBJECT 1A, ahora se dispone de dos clases de conexión adicionales: una para el DSS y otra para el TESTER.

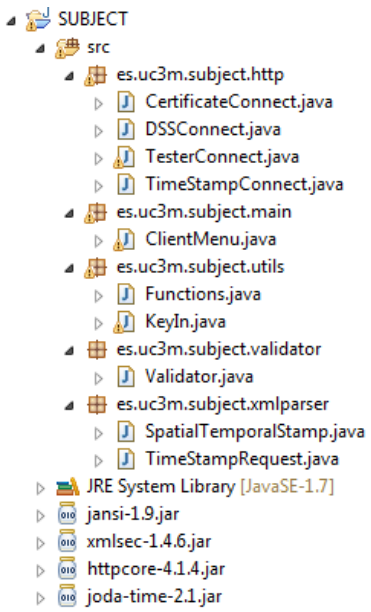


Ilustración 37 - Workspace de 1B

Además, como ya no se genera Sigma.xml desde el cliente, no es necesario disponer de una clase para ello. La estructura del módulo dentro del workspace se puede ver en la ilustración 37.

El proceso de creación del Sello Espacio-Temporal es tal y como se muestra en la ilustración 38. En cuanto a la parte de validación, el módulo actual comprueba que los resúmenes almacenados son correctos, verifica que la fecha del CET es anterior a la del ST y hace uso del DSS para que valide firmas y certificados.

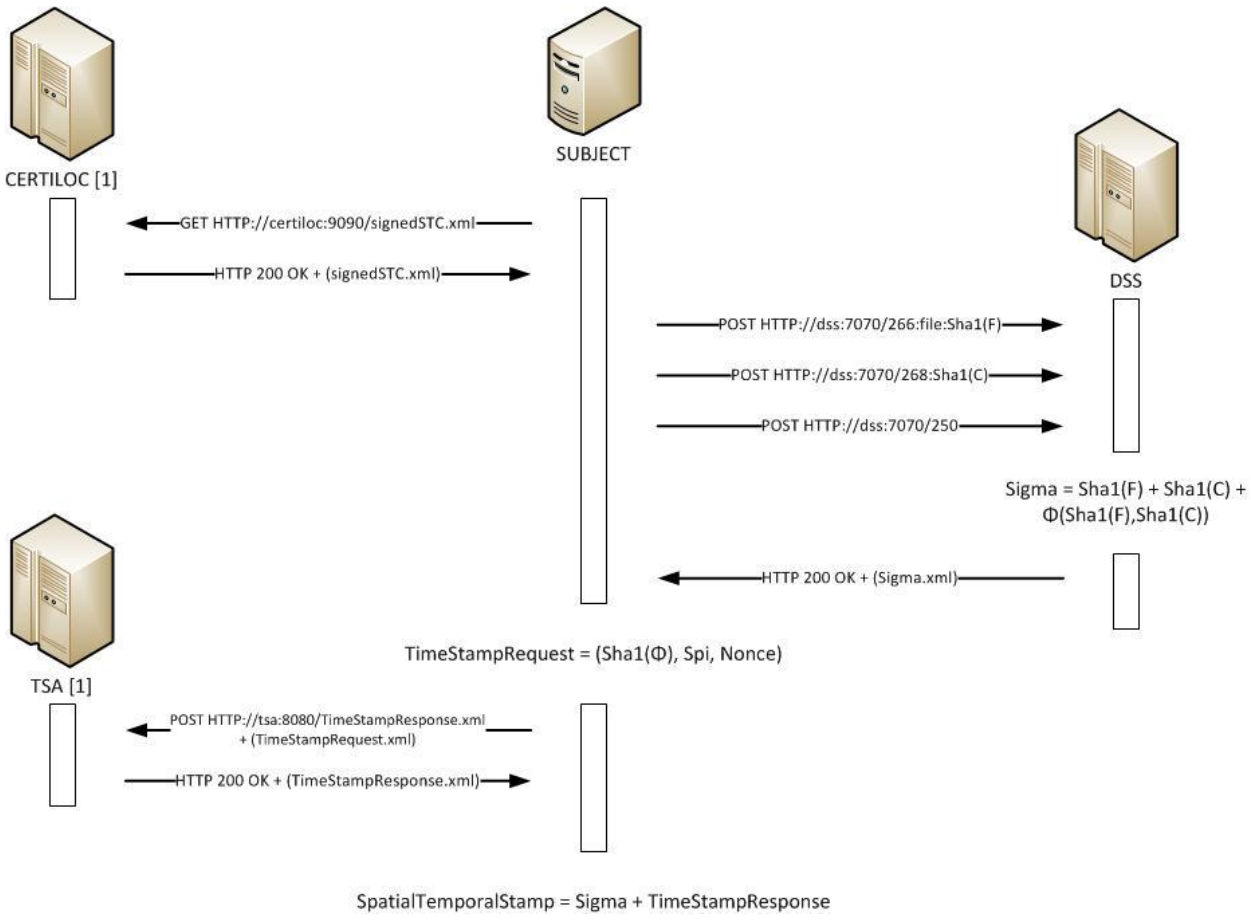


Ilustración 38 - Arquitectura del nuevo servicio de sellado espacio-temporal

Diagrama de Clases

En la ilustración 39 se puede ver el diagrama de clases del proyecto. En la tabla 55 se pueden ver con detalle dichas clases.

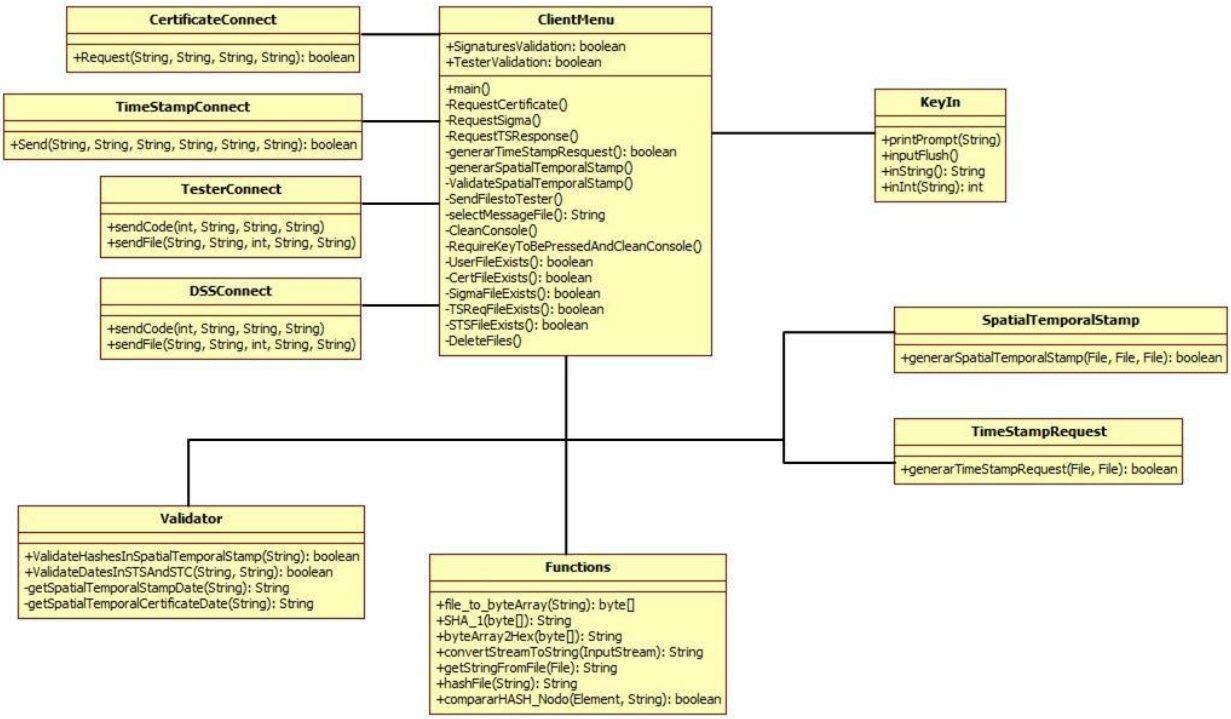


Ilustración 39 - Diagrama de clases SUBJECT 1B

CLASE	FUNCIÓN
ClientMenu	Mostrar la interfaz de control del programa, manejar las opciones del menú e interaccionar con el usuario.
KeyIn	Ayudar al usuario a interaccionar con la línea de comando.
Functions	Almacenar funciones comunes para varias clases diferentes.
CertificateConnect	Crear la conexión con el módulo CERTILOC, enviar la petición correspondiente y recibir y almacenar el certificado.
DSSConnect	Crear la conexión con el módulo DSS, enviar los ficheros, hashes y peticiones, recibir el resultado de las validaciones y recibir sigma.
TimeStampConnect	Crear la conexión con el módulo TSA, enviar la petición correspondiente y recibir y almacenar el sello temporal.
TesterConnect	Crear la conexión con el módulo TESTER, enviar los ficheros y recibir la aprobación/denegación de los mismos.
TimeStampRequest	Generar TimeStampRequest.xml
SpatialTemporalStamp	Generar SpatialTemporalStamp.xml
Validator	Validar los hashes y fechas del sello espacio-temporal.

Tabla 55 - Clases de SUBJECT 1B

Dependencia de librerías externas

En la tabla 56 se pueden ver las librerías del proyecto.

Nombre	Origen	Empaquetado	Función
Apache HttpComponents 4.1.4	http://hc.apache.org/	httpcore-4.1.4.jar	Crear las conexiones con CERTILOC, TSA y enviar/recibir ficheros. Con ambas entidades.
Jansi 1.9	http://jansi.fusesource.org/	jansi-1.9.jar	Manejar la salida por pantalla en línea de comando.
Joda Time 2.1	http://joda-time.sourceforge.net/	joda-time-2.1.jar	Calcular diferencias entre las fechas del certificado y el sello temporal.
Apache Santuario 1.4.6	http://santuario.apache.org/	xmlsec-1.4.6.jar	Manipular instancias de la clase XMLSignature poder generar y verificar firmas

Tabla 56 - Librerías de SUBJECT 1B

5.7. Módulo SUBJECT 2B

5.7.1. Diseño

Este módulo consiste en la implementación en lenguaje Java Android SDK del módulo SUBJECT 1B. Dicha implementación necesitará modificar algunas funciones de código, pues algunas de las librerías usadas en SUBJECT 1B no son compatibles con una aplicación Android.

A la hora de desarrollar la aplicación, se considera que el proceso de generación del sello espacio-temporal será transparente para los usuarios. Por ello, en esta aplicación solo existirá una opción para realizar todo el proceso, a diferencia de SUBJECT 1B donde se podía generar paso a paso.

Se decide que el nombre de la aplicación sea CERTILOC APP y que conste de una interfaz sencilla, donde aparecerán los botones necesarios para realizar todas las tareas. El objetivo principal del TFG es implementar en esta aplicación las tareas que realizaba el SUBJECT [1], por lo que no se incluirán opciones a la aplicación. Los datos de conexión HTTP irán incluidos directamente en el código, dejando como posible

mejora futura la inclusión de un menú de opciones donde poder configurar el servidor o dirección de conexión de los servicios CERTILOC, DSS, TSA y TESTER.

En lo referente a la interfaz gráfica, la aplicación costará únicamente de tres pantallas distintas:

- **Main**: donde se mostrará el menú de opciones de la aplicación.
- **File**: donde se mostrará una lista de ficheros y directorios para seleccionar el fichero sobre el que se genera el sello.
- **Info**: donde se mostrará la información del sello espacio-temporal.

A continuación se observa un boceto o *mockup* de la interfaz Main (ver ilustración 40), la interfaz File (ver ilustración 41) y la interfaz Info (ver ilustración 42).

Ilustración 40 - Boceto interfaz Main

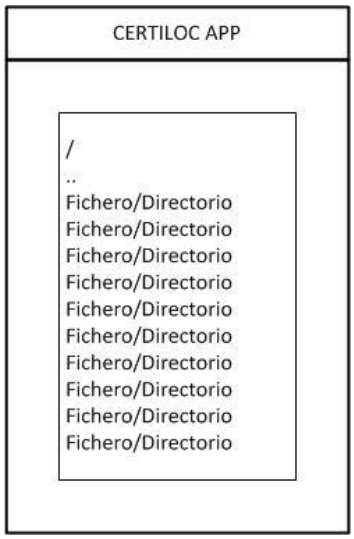


Ilustración 41 - Boceto interfaz File

Ilustración 42 - Boceto interfaz Info

Con este diseño, la generación del sello es totalmente transparente para el usuario. Además la aplicación queda con una interfaz bastante sencilla de manejar y sin necesidad de navegar a través de varias pantallas o pestañas. La ilustración 43 muestra el diagrama de flujo de iteraciones con la aplicación.

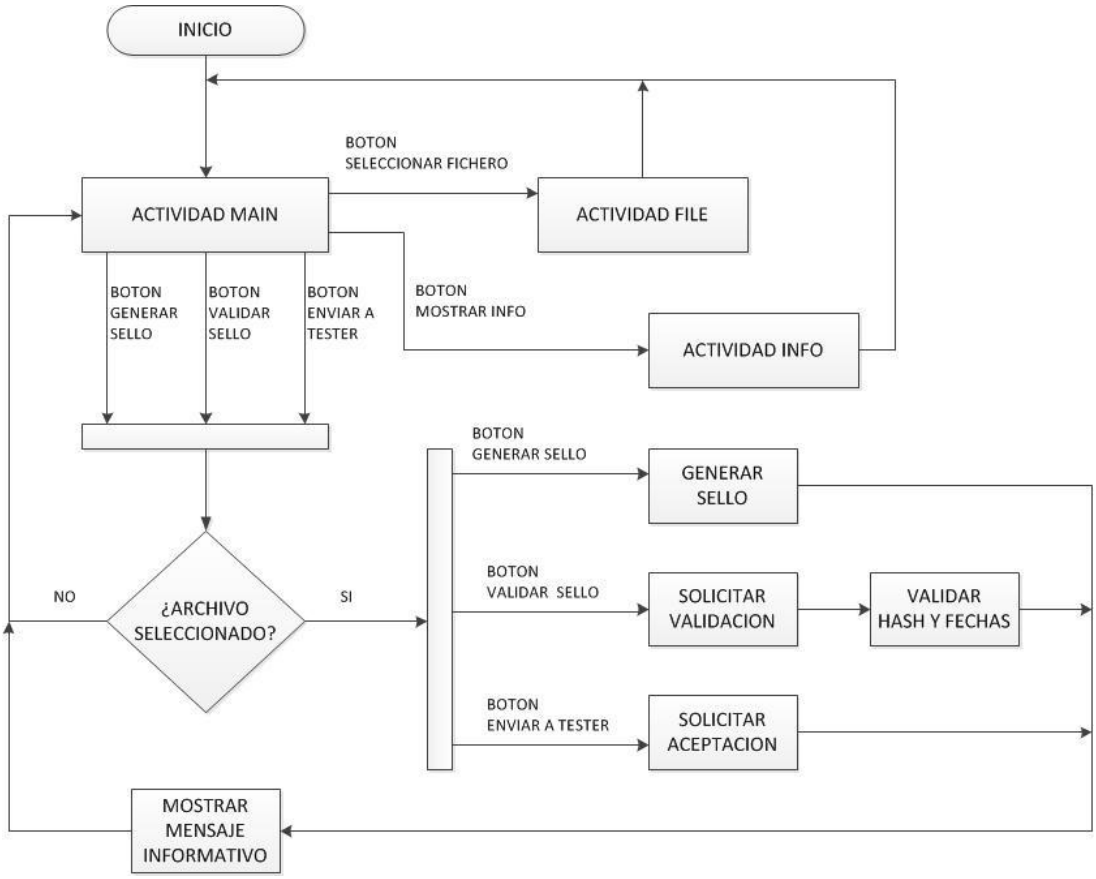


Ilustración 43 - Diagrama de flujo de SUBJECT 2B

El desarrollo del caso de uso "Mostrar información SET" incluía en este caso (dispositivo móvil) el visualizar gráficamente la interpretación de la información contenida en éste, es decir, el área geográfica donde el sujeto ha generado la firma digital sobre el documento. Sin embargo, dicha funcionalidad no pudo ser añadida a la aplicación por la incapacidad de la API Google Maps Android v2.0 (librería más actual en el momento de desarrollo del proyecto) para ejecutarse en un proyecto donde no se cargue el mapa desde el inicio de la aplicación. Se ha implementado esta funcionalidad en una aplicación distinta que se detalla en el punto 5.7.3 CERTILOC MAPS

5.7.2. Implementación

Para el desarrollo de la aplicación, se ha decidido crear tres paquetes diferentes dentro de ella para diferenciar las distintas funciones de los ficheros .java incluidos en ellos:

- **es.uc3m.certilocapp.activity**: donde se almacenarán las diferentes **activity**, que son las pantallas que poseen iteración con el usuario.
- **es.uc3m.certilocapp.service**: donde se almacenarán las clases que establecen la conexión con los distintos servicios HTTP.
- **es.uc3m.certilocapp.utils**: donde se almacenarán los generadores de ficheros XML, los validadores del sello y funciones comunes a otras clases.

La estructura del módulo dentro del workspace se puede ver en la ilustración 44.

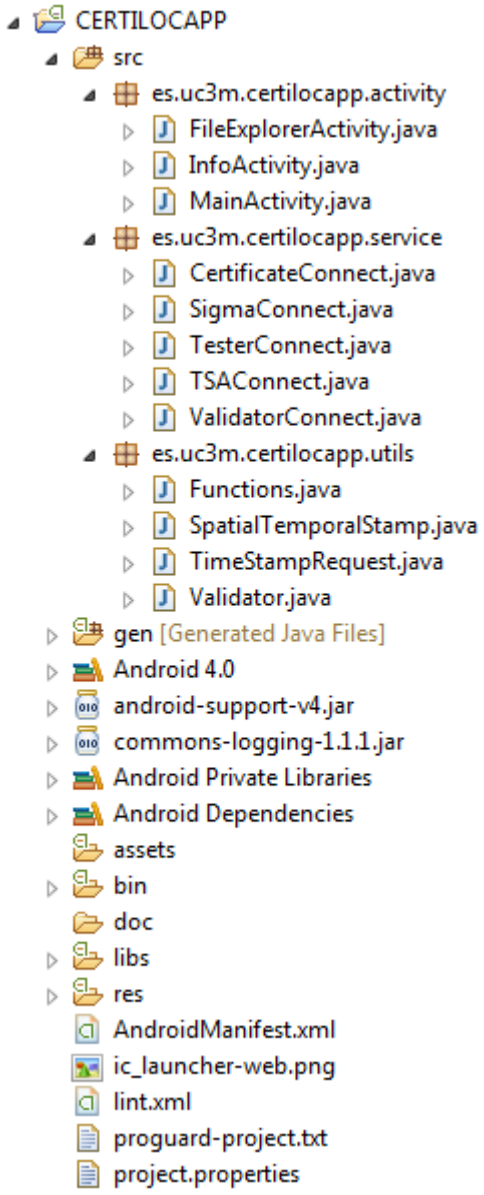


Ilustración 44 - Workspace de SUBJECT 2B

Entendiendo los conceptos básicos de Android y la documentación existente, se puede desarrollar una aplicación que cumpla las especificaciones de diseño expuestas anteriormente. A continuación se procede a explicar las distintas *activities* del proyecto.

Activity Main

Esta *activity* mostrará el menú principal de la aplicación y realizará las distintas gestiones que necesite cada opción del menú: generar documentos XML, enviar o solicitar ficheros, validar fechas, etc. La interfaz de esta *activity* puede verse en la ilustración 45.

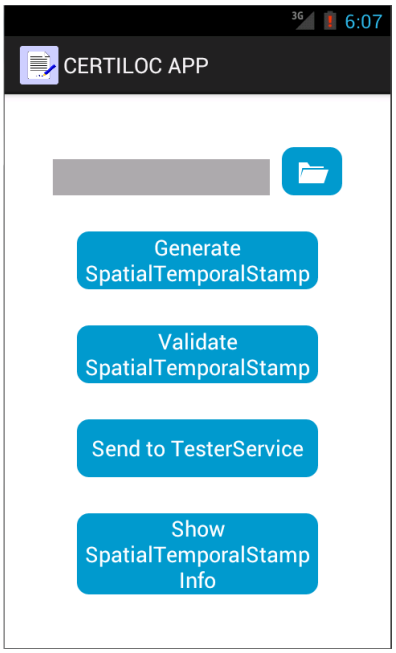


Ilustración 45 - Interfaz de Activity Main

Como se aprecia en la imagen, la interfaz posee cinco botones (en azul) y una etiqueta de texto (en gris). En la etiqueta aparecerá, una vez seleccionado, el nombre del fichero sobre el que se generará el sello espacio-temporal. Los botones ejecutarán cada uno las distintas funcionalidades de la aplicación:

- **Seleccionar archivo (símbolo carpeta)**: lanza la *activity* File.
- **Generate SpatialTemporalStamp**: ejecuta el proceso de generación del sello espacio-temporal.
- **Validate SpatialTemporalStamp**: ejecuta el proceso de validación del sello espacio-temporal.
- **Send to TesterService**: envía el fichero, certificado y sello al servicio TESTER para su aceptación.
- **Show SpatialTemporalStamp Info**: lanza la *activity* Info.

A diferencia de una aplicación Java normal, las aplicaciones Android no poseen un directorio raíz desde el que trabajar con ficheros. En necesario darle permisos a la aplicación para poder trabajar con un directorio en concreto.

En concreto, el directorio seleccionado es "/sdcard/certilocDir", donde sdcard referencia a una tarjeta de memoria externa introducida en el dispositivo, ya que no se puede dar permisos a una aplicación para guardar datos en la memoria interna del teléfono. Por ello, para que la aplicación funcione correctamente, es **necesario que el dispositivo posea una tarjeta de memoria externa**.

En esta carpeta solo se almacenarán los distintos documentos XML recibidos o generados. El fichero sobre el que se genere el sello **no será almacenado** en esta carpeta, por ello es necesario seleccionarlo siempre que se desee generar, validar o enviar a TESTER.

Para la conexión HTTP con los distintos servicios, el método de conexión es diferente al que se realiza en Java estándar. En Java estándar, se define la conexión, en la que se configura dirección (IP o nombre del host) y puerto. Posteriormente se configura: el método de conexión (POST o GET); la petición al servicio (URI) y los ficheros anexados, si se incluyeran.

En Java Android SDK, las peticiones HTTP se realizan de una manera más sencilla, tal y como se muestra a continuación:

$$HttpClient\ client\ =\ new\ DefaultHttpClient()$$

$$HttpGet\ request\ =\ new\ HttpGet(URL)\ //\ HttpPost\ request = new\ HttpPost(URL)$$

$$HttpResponse\ response\ =\ client.execute(request);$$

Donde *URL* es la dirección del servicio al que se quiere enviar la petición. Esta dirección puede ser el nombre de un host o la dirección IP del mismo, seguida de la petición al recurso. Por lo tanto, en URL debe definirse la petición exacta que se quiere realizar a la hora de realizarla. Posteriormente, se añaden los ficheros anexados si fuera el caso.

En la ilustración 46 se muestra un ejemplo de la petición al servicio TSA:

```
private static String url="http://192.168.1.21:8080/TimeStampResponse.xml";

HttpClient client = new DefaultHttpClient();

HttpPost request = new HttpPost(url);

HttpResponse response =client.execute(request);
```

Ilustración 46 - Ejemplo de conexión al módulo TSA

Debido a este sistema, fue necesario realizar el cambio en CERTILOC explicado en la sección 5.1 Módulo CERTILOC.

Activity File

Esta *activity* muestra un explorador de carpetas en el que seleccionar el fichero sobre el que se desea generar el sello espacio-temporal. La implementación de esta *activity* no está desarrollado por el autor del TFG, si no que se utilizó el explorador de carpetas utilizado en [18].

A través de ella, se selecciona navega entre los directorios del sistema operativo hasta seleccionar el fichero deseado. Entonces la aplicación almacena el nombre y ruta del fichero seleccionado para su posterior uso en las diferentes opciones del menú principal. La interfaz de esta *activity* puede verse en la ilustración 47.

Ilustración 47 - Interfaz de Activity File

Activity Info

En esta *activity* se muestra la información contenida en el sello espacio-temporal. La interfaz de esta *activity* puede verse en la ilustración 48.

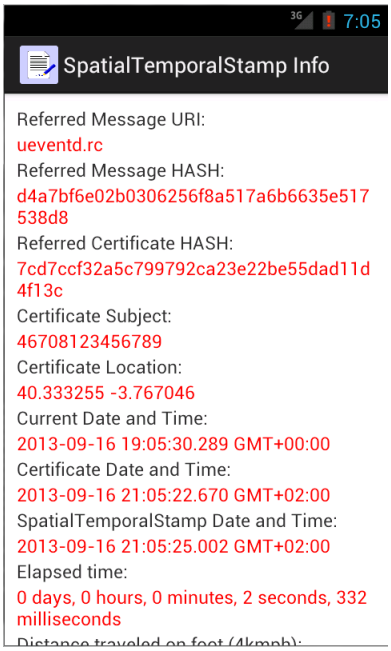


Ilustración 48 - Interfaz de Activity Info

Ya que la aplicación no permite el almacenaje de más de un sello, por no formar parte de los objetivos del TFG, no se da la opción de elegir el sello y directamente muestra la información contenida en el documento. Si no existiera ningún SET almacenado, la *activity* no se lanzaría y, en su lugar, se mostraría un mensaje informativo.

Diagramas de Clase

Al programar las *activity* de Android, se utilizan los eventos para ejecutar funcionalidades. Algunos de estos eventos son: al pulsar un botón, al cerrar la aplicación, al retornar a la pantalla anterior, al abrir la aplicación, etc. En esta aplicación principalmente se utilizan los eventos de pulsar un botón (*onClick*) y finalizar la activity (*finish*); además del evento iniciar la activity (*onCreate*) que es obligatorio de implementar.

El resto de clases que no son de tipo Activity se codifican como clases de Java estándar.

El diagrama de clases de la aplicación puede verse en la ilustración 49 y en la tabla 57 se puede ver cada clase en detalle.

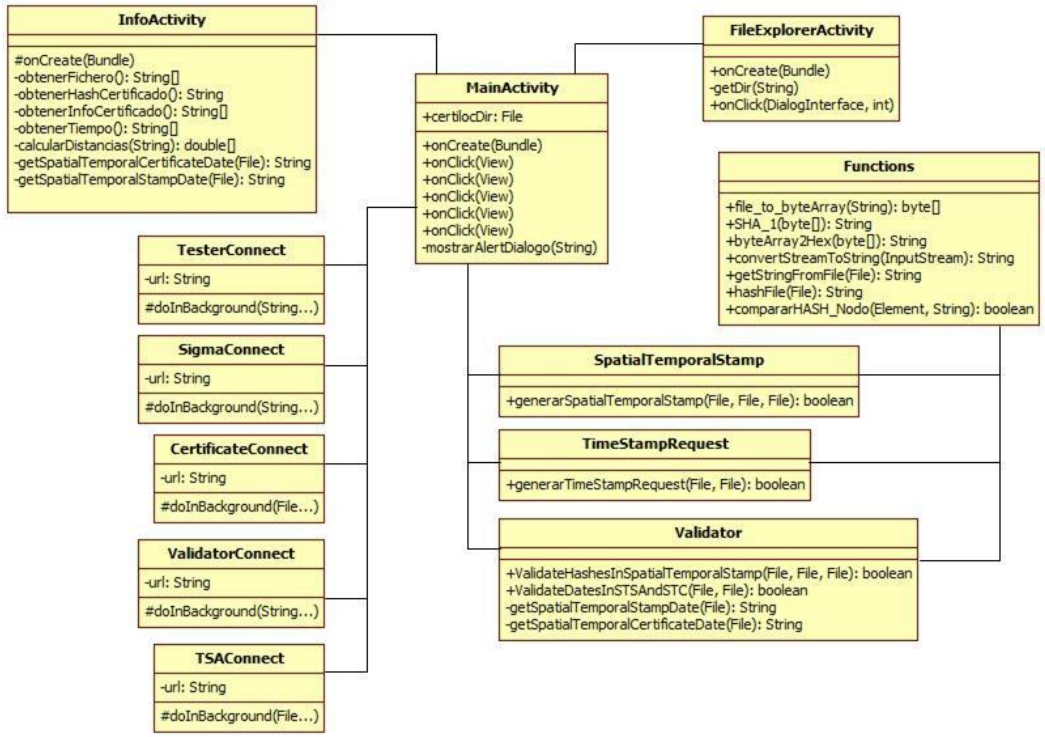


Ilustración 49 - Diagrama de clases SUBJECT 2B

CLASE	FUNCIÓN
MainActivity	Mostrar la interfaz de control del programa, manejar las opciones del menú e interaccionar con el usuario.
FileActivity	Mostrar el navegador de carpetas.
InfoActivity	Mostrar la información del sello espacio-temporal almacenado.
CertificateConnect	Crear la conexión con el módulo CERTILOC, enviar la petición correspondiente y recibir y almacenar el certificado.
SigmaConnect	Crear la conexión con el módulo DSS, enviar los hashes y solicitar y recibir sigma.
TSAConnect	Crear la conexión con el módulo TSA, enviar la petición correspondiente y recibir y almacenar el sello temporal.
ValidatorConnect	Crear la conexión con el módulo DSS, enviar los ficheros y solicitar y recibir la validación de firmas.

TesterConnect	Crear la conexión con el módulo TESTER, enviar los ficheros y recibir el resultado de la aceptación
TimeStampRequest	Generar TimeStampRequest.xml
SpatialTemporalStamp	Generar SpatialTemporalStamp.xml
Validator	Validar los hashes y fechas del sello espacio-temporal.
Functions	Almacenar funciones comunes para varias clases diferentes.

Tabla 57 - Clases de SUBJECT 2B

Dependencia de librerías externas

En la tabla 58 se pueden ver las librerías del proyecto.

Nombre	Origen	Empaquetado	Función
Android Support Library	http://developer.android.com/tools/support-library	android-support-v4.jar	Proporciona compatibilidad con versiones anteriores de Android, así como características que sólo están disponibles a través de la APIs de la librería.
Apache Commons Loggin	http://commons.apache.org/proper/commons-logging/	commons-loggin-1.1.1.jar	Sirve para realizar un log (diario) desde un programa en Java con las herramientas de Apache.

Tabla 58 - Librerías de SUBJ. MOVIL B

5.7.3. CERTILOC MAPS

Diseño

CERTILOC MAPS es una aplicación paralela a CERTILOC APP, pero que necesita que ésta segunda esté instalada para poder ejecutarse correctamente.

La funcionalidad de esta aplicación es mostrar varias áreas geográficas donde el sujeto pudo haber generado el sello espacio-temporal almacenado en el dispositivo móvil. Para calcular dichas zonas, se utiliza la fórmula de la velocidad despejando la distancia:

$$v = \frac{s}{t} \rightarrow s = v * t$$

El tiempo se obtiene al calcular la diferencia entre la fecha de generación del certificado espacio-temporal y la fecha del sello temporal. Para la velocidad se

utilizarán tres valores orientativos que consideran que el sujeto iba andando (4 km/h), en coche por ciudad (50 km/h) o en coche por carretera (120 km/h).

Con estos valores se obtiene la posible distancia máxima recorrida por el sujeto durante la generación del sello espacio-temporal. No obstante, como no se puede saber la dirección exacta del sujeto, se utilizará la distancia como el radio de la posible zona circular donde se generó y se utilizan las coordenadas contenidas en el certificado espacio-temporal como el centro de la zona.

La interfaz de la aplicación constará de una única pantalla donde se mostrará un mapa de Google Map. En el mapa se mostrará mediante iconos la localización que aparece en el certificado espacio-temporal y la localización actual del dispositivo móvil. También se mostrarán tres círculos que representarán las áreas de efecto calculadas mediante la explicación anterior. La ilustración 50 muestra un boceto o *mockup* de la interfaz.

Ilustración 50 - Interfaz de CERTILOC MAPS

Implementación

Para el desarrollo de la aplicación, se ha creado solo un único paquete, pues solo contiene una activity que implemente directamente la funcionalidad de la aplicación. En la ilustración 51 se puede observar el workspace del proyecto.

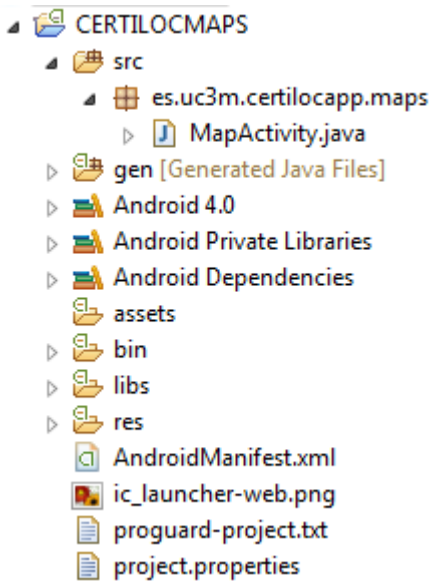


Ilustración 51 - Workspace de CERTILOC MAPS.

En esta aplicación sí se ha incluido un menú de opciones, al que se accede pulsando el botón de opciones del dispositivo. Este menú contiene las siguientes opciones:

- **Show location**: redirige la cámara a las coordenadas almacenadas en el certificado espacio-temporal.
- **Show areas**: muestra u oculta las áreas de generación del sello.
- **Normal view**: cambia el mapa a modo normal.
- **Hybrid view**: cambia el mapa a modo híbrido.
- **Map info**: muestra la leyenda de las áreas de efecto.

Por otro lado, para poder utilizar los mapas de Google en la aplicación es necesario realizar dos pasos previos:

- Instalar las librerías de Google Play service (google-play-services_lib) y ponerlas como referencias del proyecto.
- Crearse una cuenta en Google Apis [19] y configurar una clave para poder utilizar Google Maps. Esta clave estará ligada al *keystore* del entorno de desarrollo Eclipse desde el que se va a programar el proyecto.

Todos los pasos previos necesarios, así como el manejo y uso de Google Map en la aplicación, se puede observar en la referencia [20]. A continuación se puede ver un

ejemplo de la interfaz sin las áreas dibujadas (ilustración 52), con las áreas dibujadas (ilustración 53) y el menú de opciones de la aplicación (ilustración 54).

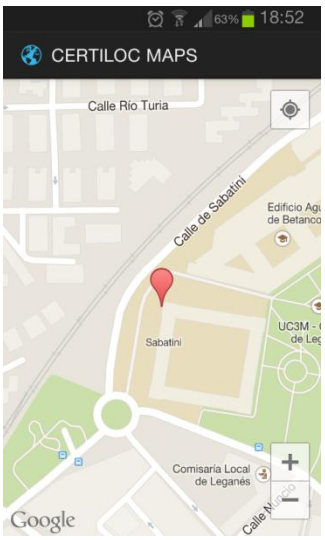


Ilustración 52 - Interfaz de CERTILOC MAPS

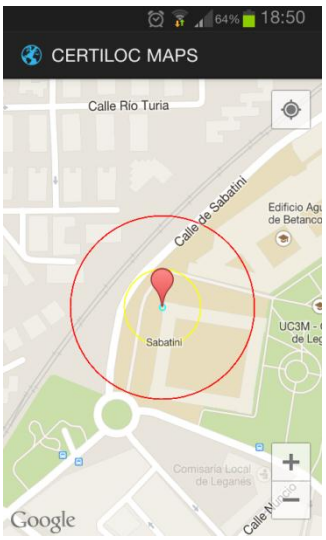


Ilustración 53 - Interfaz de CERTILOC MAPS

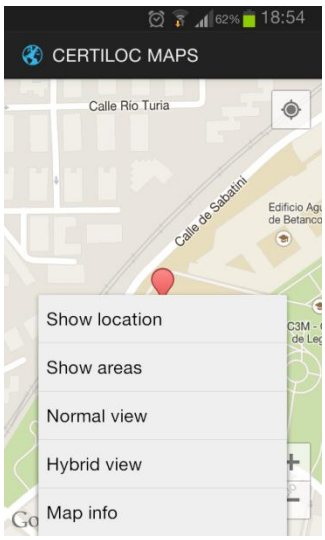


Ilustración 54 - Menú de Opciones

Diagramas de Clase

La ilustración 55 muestra el diagrama de clases de la aplicación. En este caso, consta de una sola clase.

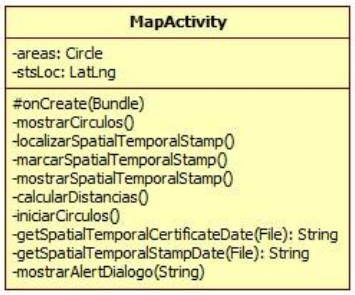


Ilustración 55 - Diagrama de clases de CERTILOC MAPS

5.8. Módulo TESTER

5.8.1. Diseño

La funcionalidad de este módulo consiste en recibir un fichero y el certificado y sello espacio-temporal generado sobre él, validar que todos los datos del sello sean correctos y devolver al cliente una respuesta sobre la aceptación o negación de los

documentos enviados. Sirve como infraestructura de prueba ante una posible implementación real del protocolo CERTILOC.

El módulo TESTER funciona como un servicio HTTP, al que un cliente se podrá conectar mediante peticiones POST a través del puerto 9000. La ilustración 56 muestra la interfaz del servicio.

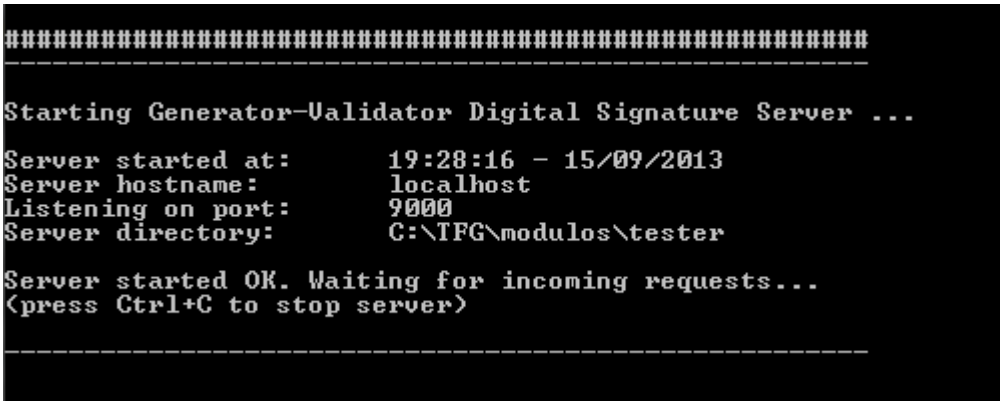


Ilustración 56 - Interfaz del servicio TESTER

Al igual que cuando se envían los ficheros al DSS para su validación, el TESTER no conoce el nombre del fichero sobre el que se genera el sello espacio-temporal; por lo que es necesario enviárselo en el transcurso de la petición.

Para ello, se ha decidido utilizar parte de los códigos de estado HTTP definidos para el DSS y descritos en el apartado 4.2 Revisión de la Arquitectura y 5.5 Módulo DSS. Ya que no son necesarios todos los códigos, los códigos a utilizar y la sintaxis de la petición serán los mostrados en la tabla 59:

Petición del Cliente	Sintaxis petición POST
Envío del fichero.	http://tester:9000/260:FileName + (FILE)
Envío del certificado.	http://tester:9000/262 + (CERT)
Envío del sello espacio-temporal.	http://tester:9000/264 + (STAMP)
Validación de los ficheros.	http://tester:9000/252

Tabla 59 - Sintaxis de peticiones al TESTER

A diferencia del DSS, el TESTER debe hacer una validación **completa** del sello espacio-temporal. Esto supone: validar firmas y certificados, comprobar que el valor de los

resúmenes sea correcto y verificar que la fecha del certificado espacio-temporal es anterior a la del sello temporal. El código para las validaciones será obtenido de los módulos DSS y SUBJECT 1B.

Una vez realizada dicha comprobación, devolverá al cliente uno de los siguientes códigos:

- 254 si todas las comprobaciones fueron correctas.
- 255 si alguna de las comprobaciones no fue correcta.
- 550 si se produce algún error en el proceso de comprobación.

La ilustración 57 muestra el proceso de comprobación de ficheros mediante TESTER.

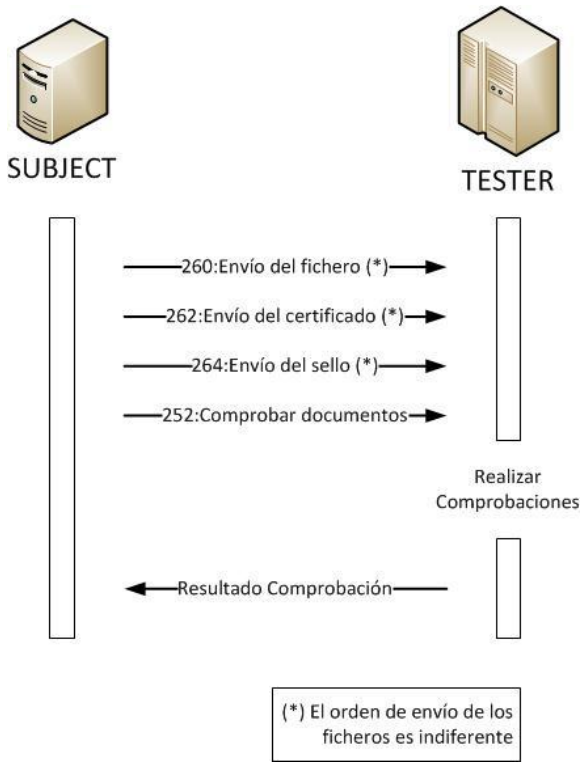


Ilustración 57 - Proceso de comprobación de documentos mediante TESTER

5.8.2. Implementación

El módulo se compone de una clase principal que implementa el servicio HTTP y las clases utilizadas para la validación en los módulos DSS y SUBJECT 1B.

El workspace del proyecto se puede observar en la ilustración 58.

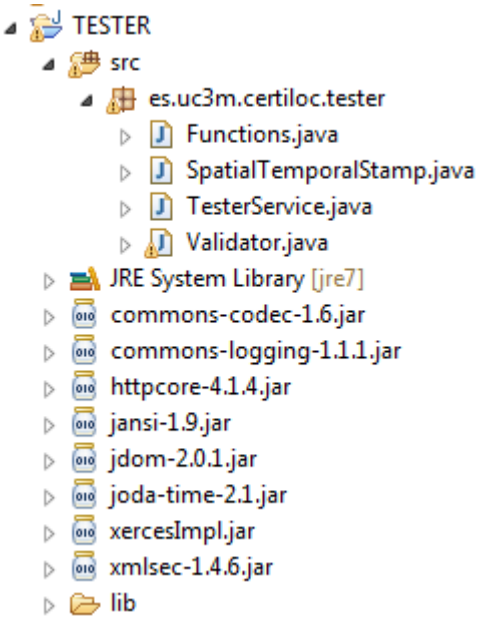


Ilustración 58 - Workspace de TESTER.

Diagrama de Clases

En la ilustración 59 se puede ver el diagrama de clases del proyecto. En la tabla 61 se pueden ver con detalle dichas clases.

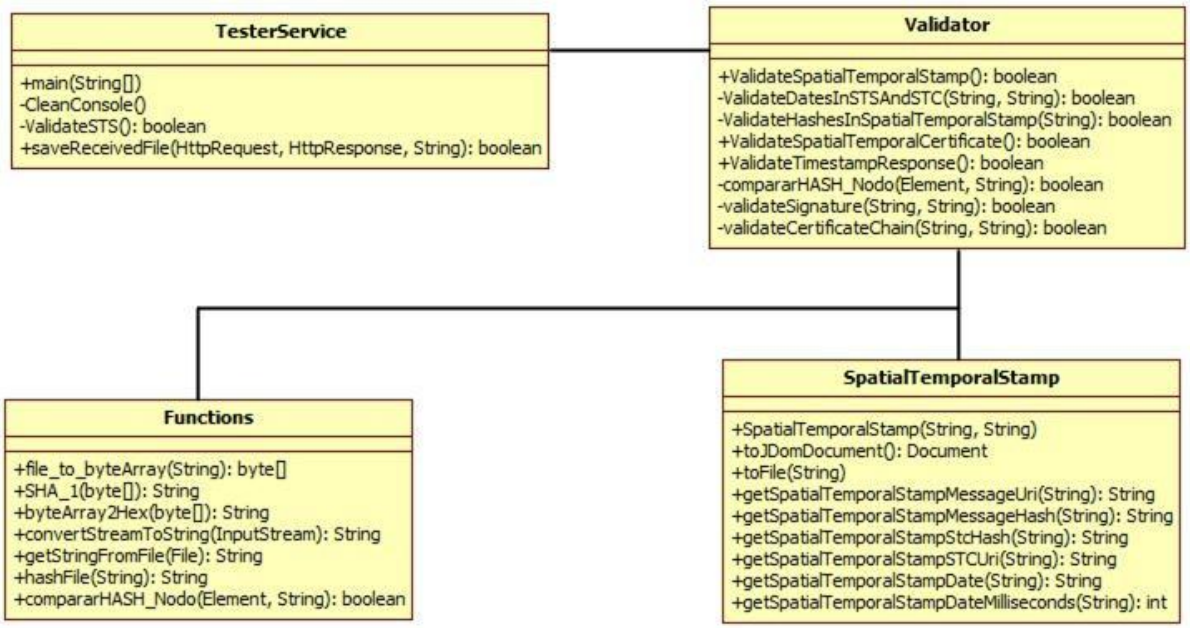


Ilustración 59 - Diagrama de clases de TESTER

CLASE	FUNCIÓN
TesterService	Mostrar la interfaz del programa, mantenerse a la espera de peticiones http y tramitar dichas peticiones.
Functions	Almacenar funciones comunes para varias clases diferentes.
Validator	Validar las firmas, certificados, hashes y fechas del sello espacio-temporal y los certificados.
SpatialTemporalStamp	Moverse a través del sello espacio-temporal para obtener los datos de las firmas y los certificados.

Tabla 60 - Clases de TESTER

Dependencia de librerías externas

En la tabla 62 se pueden ver las librerías del proyecto.

Nombre	Origen	Empaquetado	Función
Apache HttpComponents 4.1.4	http://hc.apache.org/	httpcore-4.1.4.jar	Crear las conexiones con CERTILOC, TSA y enviar/recibir ficheros. Con ambas entidades.
Jansi 1.9	http://jansi.fusesource.org/	jansi-1.9.jar	Manejar la salida por pantalla en línea de comando.
JDOM 2.0.1	http://www.jdom.org/	jdom-2.0.1.jar	Permitir el manejo de documentos XML conforme al modelo de objetos de documento (DOM).
Apache Santuario 1.4.6	http://santuario.apache.org/	xmlsec-1.4.6.jar	Manipular instancias de la clase XMLSignature poder generar y verificar firmas
Joda Time 2.1	http://joda-time.sourceforge.net/	joda-time-2.1.jar	Calcular diferencias entre las fechas del certificado y el sello temporal.
Xerces	http://www.jdom.org/	xercesImpl.jar	Librería necesaria para el funcionamiento de Jdom y otras invocaciones desde código donde se usa el DOM clásico.
Apache Commons Codec 1.6	http://commons.apache.org/codec/	commons-codec-1.6.jar	Permitir transformar un resumen en formato array de bytes a hexadecimal
Apache Commons Loggin	http://commons.apache.org/proper/commons-logging/	commons-loggin-1.1.1.jar	Sirve para realizar un log (diario) desde un programa en Java con las herramientas de Apache.

Tabla 61 - Librerías de TESTER

6. PRUEBAS

En este apartado se muestran los distintos resultados tras la realización de las pruebas definidas en el punto 4.4 Plan de Pruebas con el fin de garantizar que el sistema cumple con el objetivo de este TFG.

Las pruebas podrán tener dos tipos de resultados:

- **Superada**: Se han realizado todos los pasos descritos en la prueba y el resultado obtenido es el esperado.
- **No superada**: Se han podido realizar todos los pasos descritos en la prueba y el resultado obtenido no es el esperado. Adicionalmente, las pruebas en las que no se hayan podido ejecutar todos los pasos también serán calificadas como no superadas.

A continuación se muestra la tabla 61, donde se puede ver el resultado de cada prueba. Se ha añadido una columna adicional para indicar si la prueba se realizaba sobre SUBJECT 1B o SUJECT 2B.

ID	Resultado		Entidad de prueba	
	Superada	No superada	SUBJECT 1B	SUBJECT 2B
PR001	X			X
PR002	X			X
PR003	X			X
PR004	X		X	
PR004	X			X
PR005	X		X	
PR005	X			X
PR006	X		X	
PR006	X			X
PR007	X		X	

PR007	X		X
PR008	X		X
PR009	X		X
PR010	X		X
PR011	X	X	
PR011	X		X
PR012	X	X	
PR012	X		X
PR013	X		X
PR014	X		X
PR015	X	X	
PR015	X		X
PR016	X	X	
PR016	X		X
PR017	X		X
PR018	X		X
PR019	X	X	
PR019	X		X
PR020	X		X
PR021	X		X
PR022	X		X
PR023	X		X

Tabla 62 - Resultado de las pruebas

7. CONCLUSIONES Y LÍNEAS FUTURAS

En este apartado se exponen, por este orden, las dificultades del proyecto, las conclusiones sobre el resultado obtenido y, por último, las líneas futuras de trabajo derivadas de este TFG.

7.1. Dificultades del proyecto

Partiendo del hecho de que migrar un sistema de una plataforma a otra distinta no suele ser, por norma general, una tarea sencilla; que la plataforma destino de esa migración sea Android aumenta la complejidad de la tarea.

Android es un sistema operativo joven (la primera versión salió al mercado en 2008 [23]) que aún no ha sido explotado en su mayoría. Y aunque es un sistema operativo potente, aún no alcanza las capacidades de los sistemas operativos de ordenador (como Windows, iOS o Linux), por la sencilla razón de que el dispositivo donde se implantará el sistema tampoco tiene las mismas capacidades que un ordenador.

Estas capacidades limitadas impiden que sea sencillo migrar una aplicación Java estándar a su homónimo en Android, Java Android SDK. Librerías o componentes no soportados por dispositivos móviles suponen rediseñar una aplicación (o incluso reescribirla desde cero).

Siguiendo con las dificultades encontradas a lo largo de este TFG, cabe mencionar especialmente al estándar de firma digital XMLDSig. Por un lado, es un estándar potente que permite generar firmas de una manera rápida bajo una estructura fácilmente aplicable a cualquier entorno de programación. Por otro lado, su complejidad es igual o mayor que su potencia, pues generar una firma digital siguiendo este estándar sin utilizar las librerías correspondientes es muy complejo.

Uniendo las dos dificultades ya mencionadas se llega al que ha sido el mayor problema surgido a lo largo de este TFG, la incapacidad de Android para poder ejecutar los componentes necesarios para realizar firmas digitales XMLDSig. Esto ha

provocado, en primer lugar, una replanificación completa del proyecto, teniendo que volver a analizar y estudiar las posibles soluciones para dicho problema. Además, ha implicado la inclusión de una nueva entidad al sistema, el DSS, que para futuros proyectos basados en este TFG conllevará el incluirle diversas medidas de seguridad que no han sido implementadas por no formar parte de los objetivos.

7.2. Resultado obtenido

En lo referente a la calidad del resultado final del proyecto, se puede asegurar que el **software desarrollado satisface plenamente los objetivos principales del TFG**.

Por primera vez se intentaba implementar en una plataforma móvil el sistema de generación y validación de sellos espacio-temporales de CERTILOC. Y, aunque han surgido diversas problemas a lo largo del desarrollo de la aplicación, se puede considerar que ésta primera aproximación del proyecto CERTILOC al mundo de las plataformas digitales ha sido un éxito. El sistema desarrollado no solo permite generar un sello espacio-temporal desde un dispositivo con sistema operativo Android, sino que, además, lo hace en una arquitectura similar y compatible con los trabajos previos del proyecto CERTILOC.

Por otro lado, otro avance dentro del proyecto de investigación CERTILOC es la primera incursión de un servicio destinatario del SET, en este TFG denominado TESTER. En proyectos previos se ha mencionado que CERTILOC (como conjunto de servicios) sirve como tercero de confianza a la hora de acreditar que un sujeto realiza una firma en determinadas condiciones espacio-temporales ante un destinatario final. Sin embargo, no ha sido hasta este TFG cuando se ha implementado una primera versión de dicho destinatario, permitiendo aproximarse más a una implantación completa del proyecto CERTILOC.

7.3. Líneas futuras de trabajo

Ya que el objetivo establecido del TFG era la adaptación del módulo cliente (SUBJECT) a un dispositivo móvil, hay muchas medidas que no se han tenido en cuenta a la hora de implementar dicho módulo y que deberán abordarse en trabajos futuros. Estas medidas son, principalmente, de seguridad; puesto que a la hora de desarrollar esta primera versión de la aplicación se tuvo en cuenta la funcionalidad y no la seguridad. Por ello, como una primera enumeración de líneas futuras, se tendría:

- Modificación de las conexiones del cliente con los distintos módulos del proyecto (CERTILOC, TSA, DSS y TESTER) para implementarlas **conexiones seguras** (por ejemplo, conexiones HTTPS).
- Modificación del servicio DSS para que solicite **autenticación** al conectarse un cliente y **gestione** los certificados de firma del cliente.
- Modificación de la aplicación cliente para incluir en la firma digital generada alguna prueba criptográfica que permita **verificar a un tercero que fue el cliente quien solicitó dicho servicio**.

Por otro lado, en el ámbito de la tecnología Android, han surgido diversos problemas a lo largo del proyecto que han necesitado de una solución alternativa. Partiendo de estos problemas se podría mencionar como líneas futuras:

- Desarrollo de una aplicación Android que **no necesite del servicio ofrecido por el DSS para la generación y validación de firmas digitales**. Esta opción solo sería posible si se realiza alguna actualización en el sistema operativo Android que permita ejecutar las librerías necesarias para generar y validar firmas digitales.
- Desarrollo de una aplicación que **ejecute conjuntamente las funcionalidades de CERTILOC APP y CERTILOC MAPS**. Igual que en el caso anterior, con las implementaciones actuales de Android no se permite ejecutar la funcionalidad de Google Maps en la aplicación CERTILOC APP.

Por último, cabría destacar la opción de modificar la arquitectura actual para permitir conexiones múltiples de varios sujetos simultáneamente. Actualmente, tanto en el sistema generado en este TFG como en [1] distintos servicios (CERTILOC, TSA, DSS y TESTER) sobrescriben los ficheros existentes al generar los nuevos. Esto impide que dos sujetos puedan realizar peticiones simultáneas, pues podrían enviarse datos incorrectos. Se debería de modificar los distintos servicios para, de algún modo, permitir que se reciban peticiones de distintos sujetos y tramitarlas correctamente.

BIBLIOGRAFÍA Y REFERENCIAS

Tesis Doctorales y Proyectos Fin de Carrera

[1] Raúl David Martínez Calmaestra. Análisis, diseño e implementación de mejoras en el servicio de sellado espacio-temporal de CERTILOC. Proyecto Fin de Carrera. Universidad Carlos III de Madrid. 2012.

[2] Álvaro Gascón y Marín de la Puente. Implementación de protocolos de sellado temporal y sellado espacio-temporal en XML para CERTILOC. Proyecto de Fin de Carrera. Universidad Carlos III de Madrid. 2008.

[3] Ana Isabel González-Tablas Ferreres. Arquitectura y mecanismos para la provisión de servicios de acreditación y sellado espacio-temporal. PhD thesis. Universidad Carlos III de Madrid. 2005.

[4] J.M de Fuentes García-Romero de Tejada. Diseño e implementación del sistema de localización de dispositivos móviles con conectividad limitada dotados de receptor GPS para certiloc. Proyecto de Fin de Carrera. Universidad Carlos III de Madrid, 2007.

[5] José Carlos Calvo Martínez. Diseño e Implementación de la plataforma base de CERTILOC y del servicio de certificación espacio-temporal. Proyecto de Fin de Carrera. Universidad Carlos III de Madrid, 2007.

[6] John Páter Martínez de Leiva. Diseño e Implementación del Sistema de Políticas de Privacidad para el proyecto CERTILOC. Proyecto de Fin de Carrera. Universidad Carlos III de Madrid, 2009.

[7] Johanna Gallo Martínez. Diseño e implementación de los servicios de seguridad y de administración de entidades del sistema CERTILOC. Proyecto de Fin de Carrera. Universidad Carlos III, 2008.

Normas y Leyes

[8] W3C. XML-Signature syntax and processing. W3C Recommendation, 10 June 2008.
http://www.w3.org/TR/xmldsig-core/

[9] XML-Signature Syntax and Processing
http://datatracker.ietf.org/doc/rfc3275/

[10] Ley 59/2003, de 19 de diciembre, de firma electrónica.
http://noticias.juridicas.com/base_datos/Admin/l59-2003.html

[11] Ley General de Telecomunicaciones
http://civil.udg.es/normacivil/estatal/contract/l32-03.htm

[12] Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-22440

[13] ORDEN EHA/3636/2005, de 11 de noviembre, por la que se crea el registro telemático del Ministerio de Economía y Hacienda.
http://www.boe.es/diario_boe/txt.php?id=BOE-A-2005-19325

Páginas o documentos electrónicos en la red

[14] Apache Santuario
http://santuario.apache.org

[15] Internet Security Glossary, Version 2
http://tools.ietf.org/html/rfc4949

[16] Stack OverFlow
www.stackoverflow.com

[17] Códigos de estado HTTP
https://support.google.com/webmasters/answer/40132?hl=es

[18] Buscar, seleccionar y subir archivos desde una aplicación Android
http://androidsensei.net/aprende-a-subir-archivos-desde-tu-aplicacion-android-a-cualquier-lugar/

[19] Google Apis
https://code.google.com/apis

[20] Android y Google Maps v2 I: básico
http://directoandroid.es/2013/04/01/android-y-google-maps-v2-i-basico/

[21] IDC: Android y Windows Phone ganan cuota de mercado, iOS y BlackBerry la pierden
http://www.xataka.com/moviles/idc-android-y-windows-phone-ganan-cuota-de-mercado-ios-y-blackberry-la-pierden

[22] XML Digital Signature API
http://docs.oracle.com/javase/6/docs/technotes/guides/security/xmldsig/XMLDigitalSignature.html

[23] Announcing the Android 1.0 SDK, release 1
http://android-developers.blogspot.in/2008/09/announcing-android-10-sdk-release-1.html

[24] PKCS #7: Cryptographic Message Syntax
http://tools.ietf.org/html/rfc2315

[25] Enhanced Security Services for S/MIME
http://www.ietf.org/rfc/rfc2634.txt

[26] Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms.
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54788

[27] (TSP) (RFC 3161) - IETF
http://www.ietf.org/rfc/rfc3161.txt

ANEXOS

Apéndice A: Manual de Usuario

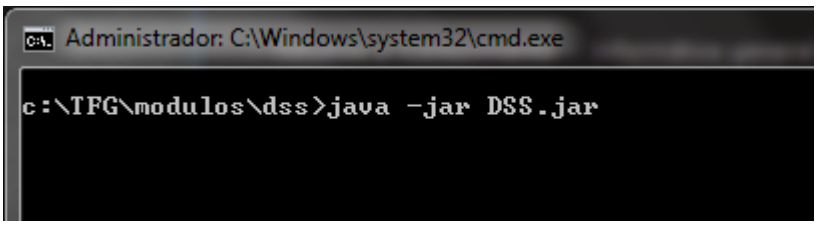
En este manual se indican los pasos necesarios para utilizar las aplicaciones CERTILOC APP y CERTILOC MAPS, y para arrancar los módulos DSS y TESTER. Para arrancar los módulos CERTILOC y TSA, se debe mirar los Anexos de [1], pues el método de arranque no ha cambiado.

Es importante recalcar que para que CERTILOC APP funcione correctamente los cuatro módulos CERTILOC, TSA, DSS y TESTER deben estar arrancados previamente en una ventana de consola. Dicha ventana debe tener, como mínimo, tener las siguientes características:

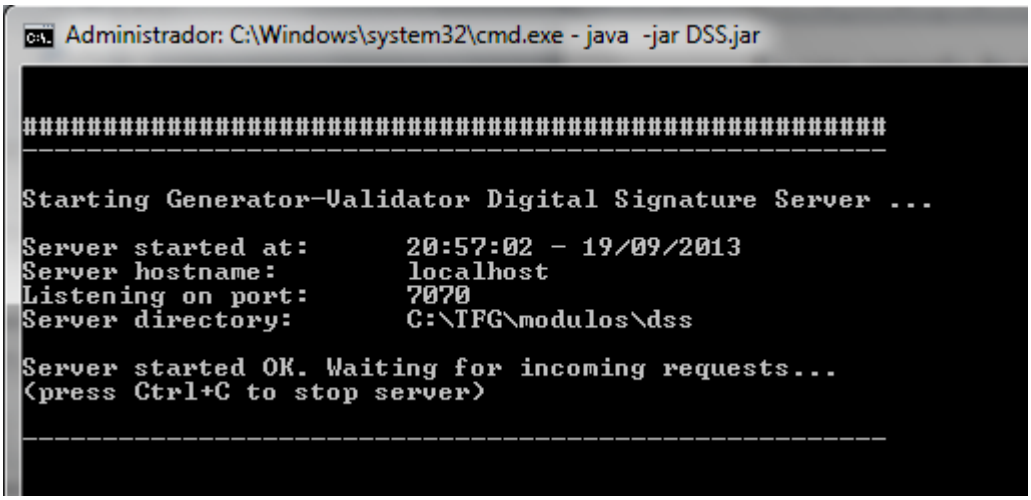
- Fuente de mapa de bits, tamaño 8x12
- Tamaño del búfer de pantalla: 137 ancho, 300 alto.
- Tamaño de la ventana: 137 ancho, 59 alto.

Arranque del servidor DSS.

1. En una consola de símbolo del sistema, dirigirse a la carpeta que contenga el proyecto y teclear el comando: java –jar DSS.jar

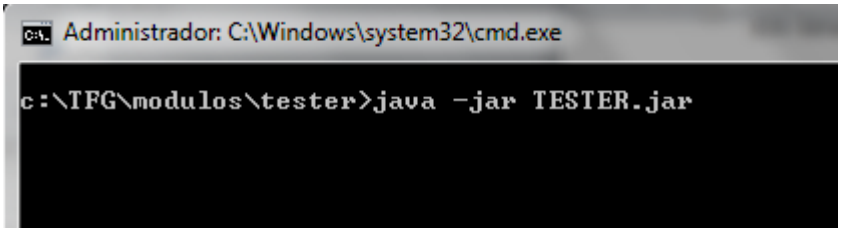


2. Comprobar que el contenido de la consola se borra y en su lugar aparece la interfaz del servidor con el mensaje *Server started OK*.

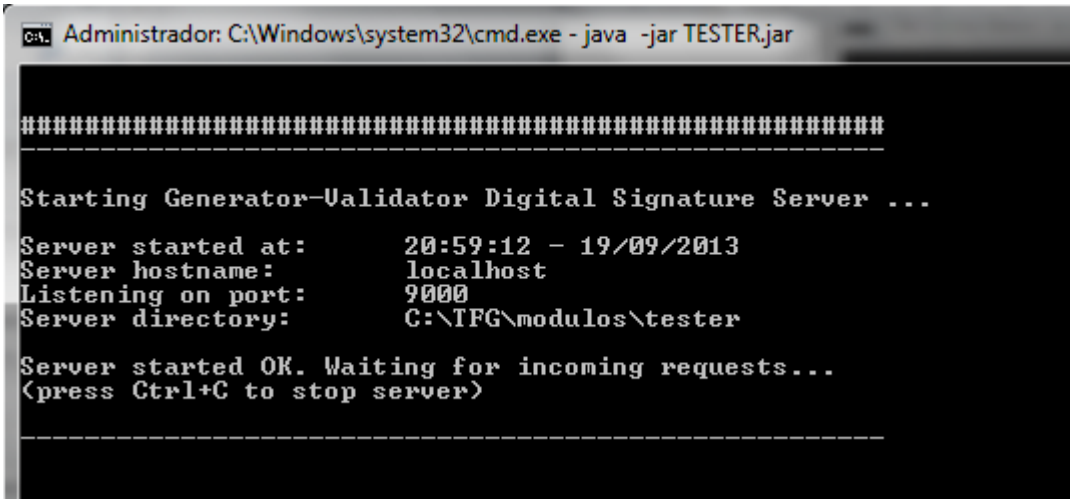


Arranque del servidor TESTER.

1. En una consola de símbolo del sistema, dirigirse a la carpeta que contenga el proyecto y teclear el comando: java –jar TESTER.jar

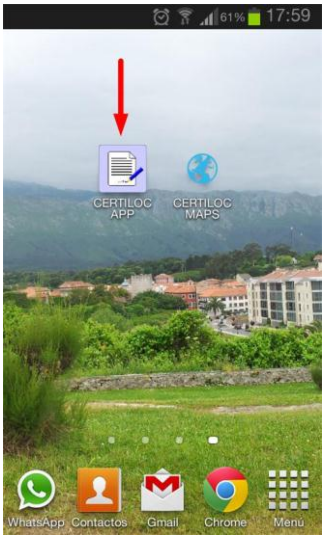


2. Comprobar que el contenido de la consola se borra y en su lugar aparece la interfaz del servidor con el mensaje *Server started OK*.

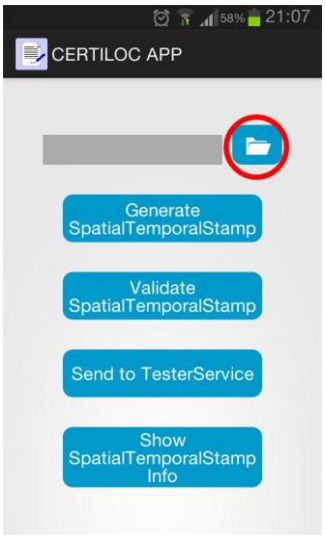


Proceso de generación de un SET mediante CERTILOC APP.

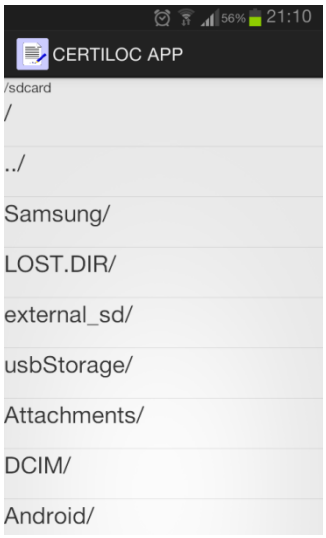
1. Una vez arrancados los servicios CERTILOC, TSA y DSS, iniciar la aplicación CERTILOC APP pulsando el icono de la aplicación.



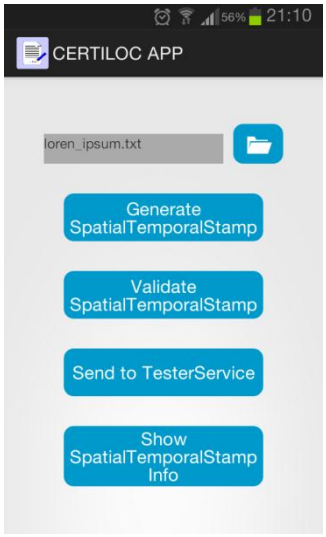
2. Pulsar en el botón *Seleccionar archivo*, situado arriba a la derecha y representado con el símbolo de una carpeta abierta.



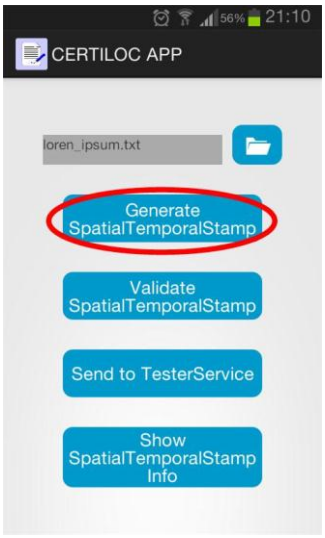
3. Navegar por el explorador de archivos hasta encontrar el archivo deseado. Al entrar en una carpeta, las dos primeras filas cambiaran por los símbolos "/" y "../" respectivamente. El primer símbolo hace referencia a la carpeta raíz del sistema operativo, abierta por defecto por el explorador. El segundo símbolo hace referencia a la carpeta superior.



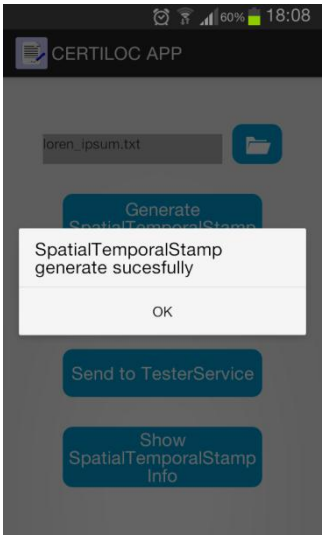
4. Una vez seleccionado el archivo, confirmar que aparece el nombre del mismo en el recuadro gris situado arriba a la izquierda, justo al lado del botón *Seleccionar archivo*.



5. Pulsar en *Generate SpatialTemporalStamp* para iniciar el proceso de generación del SET.

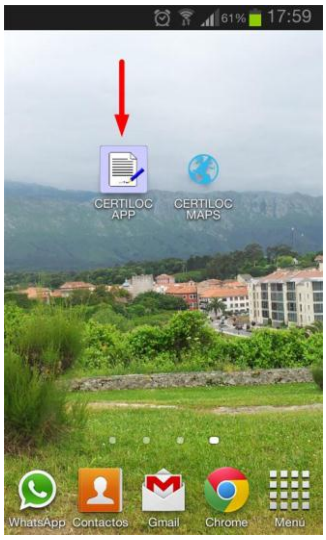


6. Una vez acabado el proceso de generación, aparecerá un mensaje informativo por pantalla. Pulsar *OK* para finalizar el proceso.

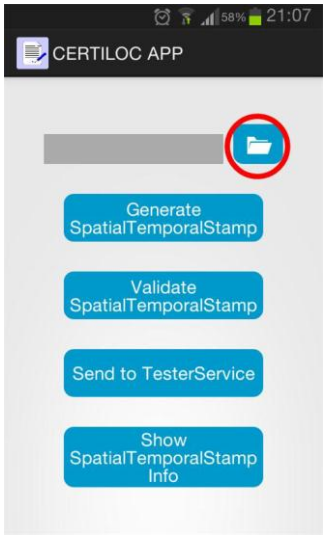


Proceso de validación de un SET mediante CERTILOC APP.

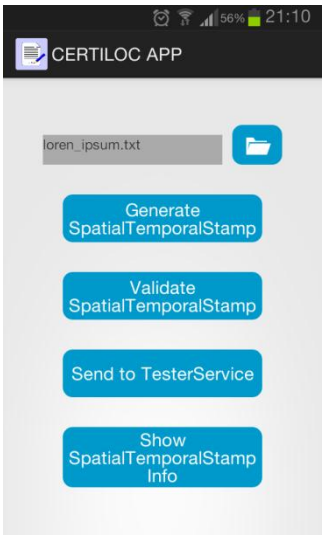
1. Una vez arrancados el servicio DSS, iniciar la aplicación CERTILOC APP pulsando el icono de la aplicación.



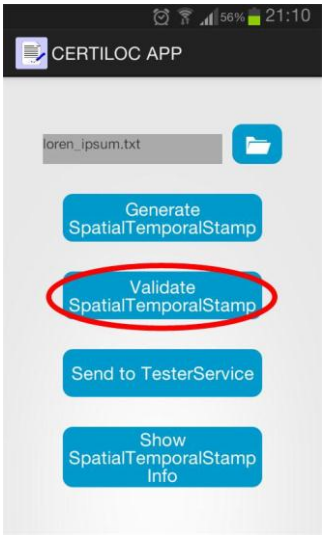
2. Pulsar en el botón *Seleccionar archivo*, situado arriba a la derecha y representado con el símbolo de una carpeta abierta.



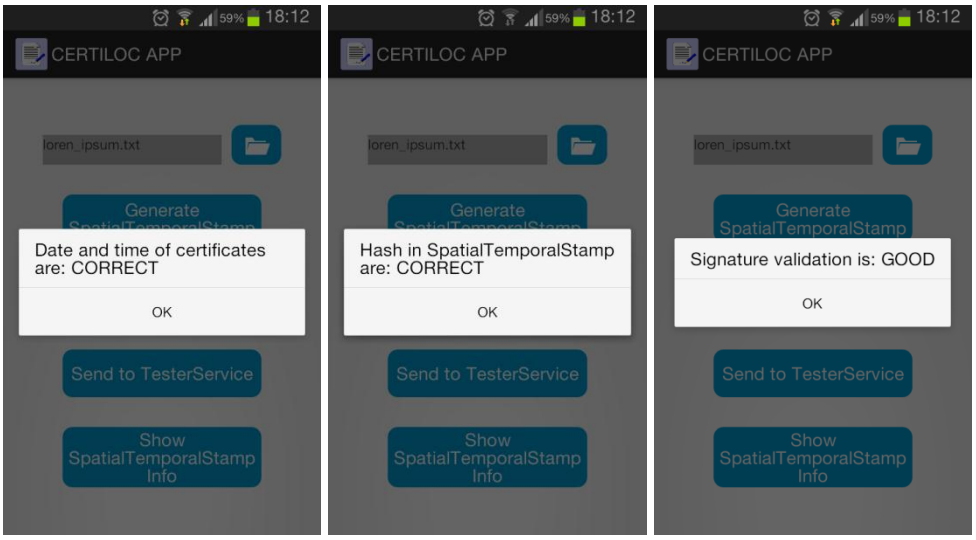
3. Navegar por el explorador de archivos hasta encontrar el **archivo sobre el que se generó el SET**. Es **imprescindible** que el fichero correcto este seleccionado.
4. Una vez seleccionado el archivo, confirmar que aparece el nombre del mismo en el recuadro gris situado arriba a la izquierda, justo al lado del botón *Seleccionar archivo*.



5. Pulsar en *Validate SpatialTemporalStamp* para iniciar el proceso de validación del SET.

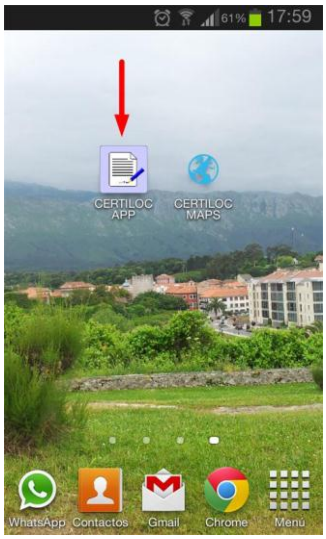


6. Una vez acabado el proceso de validación, aparecerá varios mensajes informativos por pantalla indicando el resultado de la validación de firmas, fechas y hashes. Pulsar *OK* en cada ventana para finalizar el proceso.

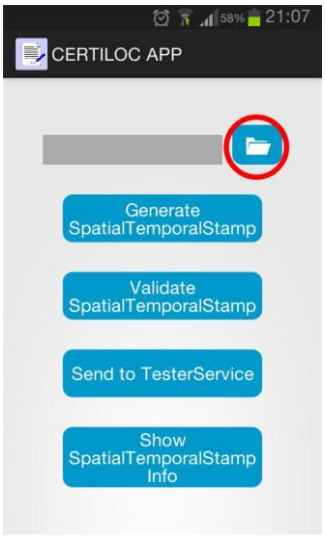


Proceso de envío de ficheros a TESTER.

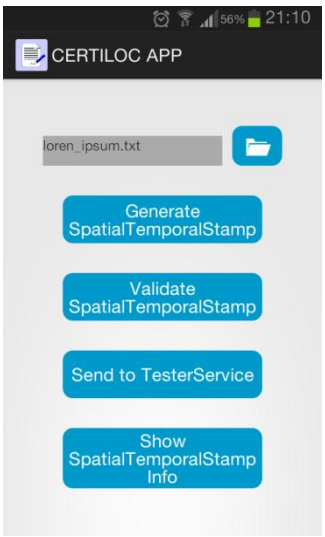
1. Una vez arrancados el servicio TESTER, iniciar la aplicación CERTILOC APP pulsando el icono de la aplicación.



2. Pulsar en el botón *Seleccionar archivo*, situado arriba a la derecha y representado con el símbolo de una carpeta abierta.

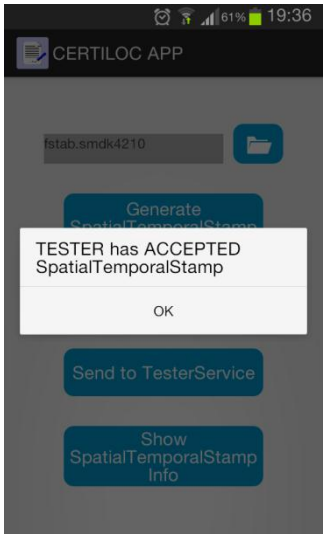


3. Navegar por el explorador de archivos hasta encontrar el **archivo sobre el que se generó el SET**. Es **imprescindible** que el fichero correcto este seleccionado.
4. Una vez seleccionado el archivo, confirmar que aparece el nombre del mismo en el recuadro gris situado arriba a la izquierda, justo al lado del botón *Seleccionar archivo*.



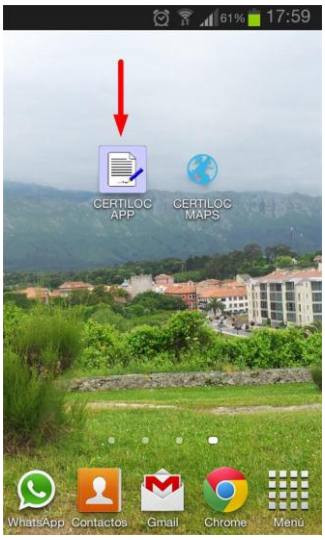
5. Pulsar en *Send to TesterService* para iniciar el proceso de aceptación de ficheros.

6. Una vez acabado el proceso de aceptación, aparecerá un mensaje informativo sobre el resultado de la aceptación de ficheros. Pulsar *OK* para finalizar el proceso.

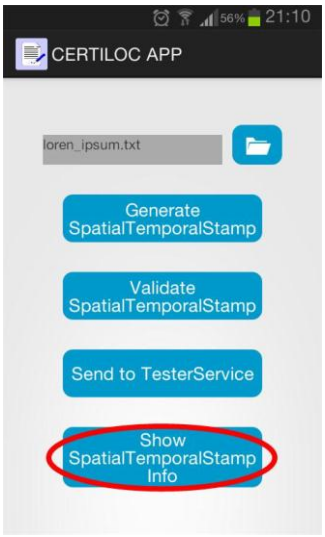


Proceso de muestra de información del SET.

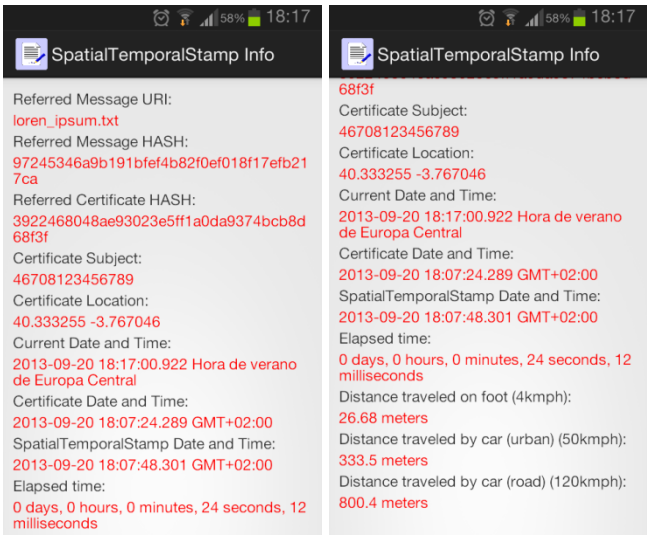
1. Iniciar la aplicación CERTILOC APP pulsando el icono de la aplicación.



2. Pulsar en *Show SpatialTemporalStamp Info*.

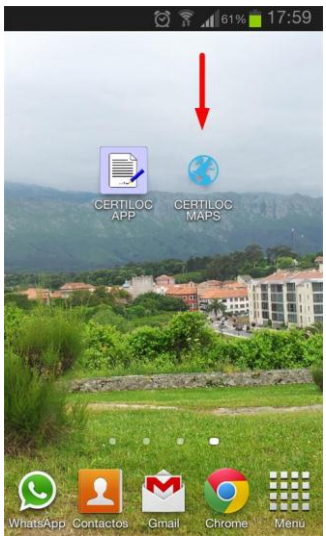


3. Aparecerá una pantalla nueva con la información del SET. Arrastrar la pantalla arriba y abajo para poder ver la información al completo. Pulsar el botón *Volver* del dispositivo para salir.

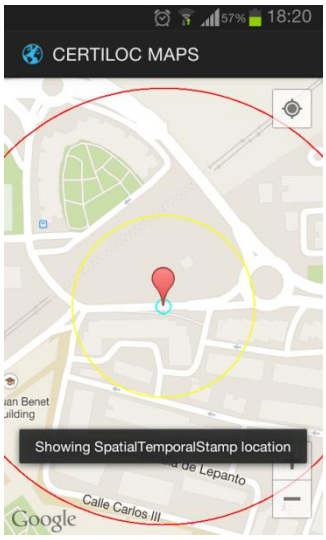


Proceso de muestra de áreas del SET mediante CERTILOC MAPS.

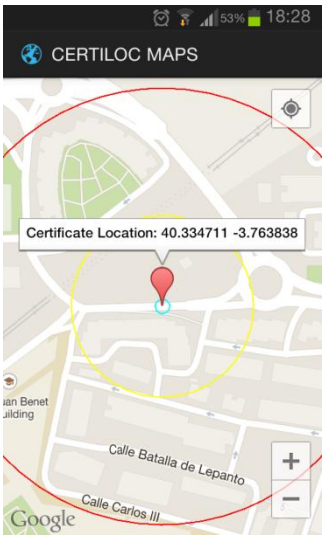
1. Iniciar la aplicación CERTILOC MAPS pulsando el icono de la aplicación.



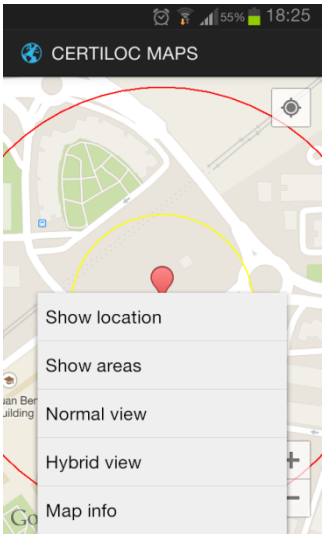
2. La aplicación realizará automáticamente el cálculo del tiempo entre CET y ST y la distancia de las áreas.



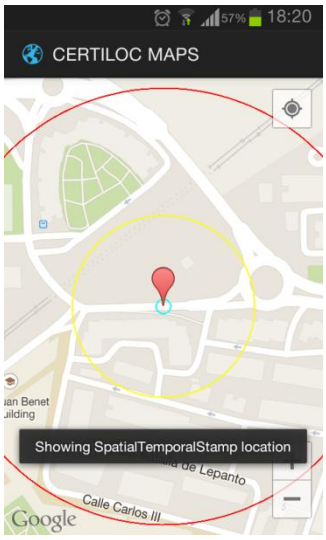
3. Pulsar el icono representativo del mapa para ver un rótulo con las coordenadas almacenadas en el CET. Pulsar en cualquier parte de la pantalla para quitar el rótulo.



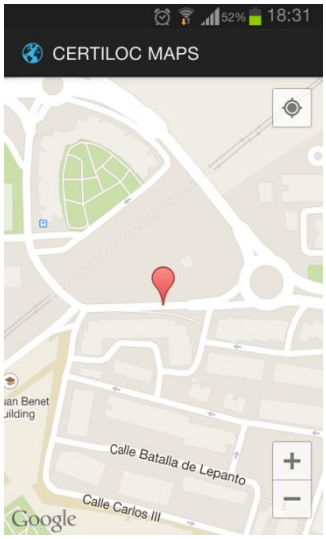
A continuación se explican el menú Opciones de la aplicación, al cual se puede acceder pulsando el botón *Opciones* del dispositivo:



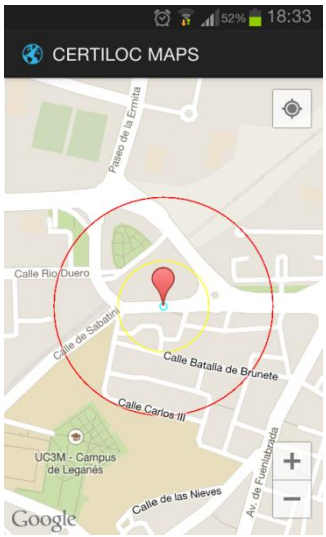
a) Pulsar *Show location* para que el mapa centre la vista en las coordenadas almacenadas en el CET.



b) Pulsar *Show areas* para que se muestren o se oculten los círculos representativos de las áreas.

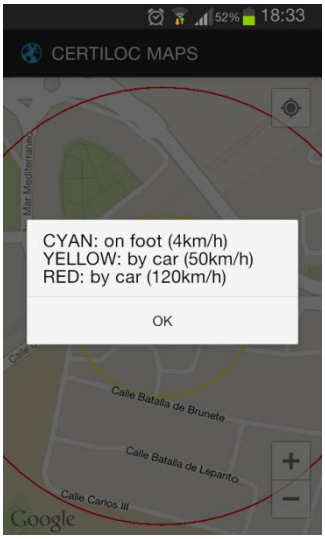


c) Pulsar *Normal view* para cambiar la vista del mapa a modo normal.



d) Pulsar *Hybrid view* para cambiar la vista del mapa a modo hibrido.

e) Pulsar *Map info* para mostrar la leyenda del mapa. Pulsar OK para cerrar la ventana.



Apéndice B: Manual de Instalación

En este manual se indican los pasos necesarios para instalar la aplicación CERTILOC APP en un dispositivo móvil. Para instalar la aplicación CERTILOC MAPS se debe seguir los mismos pasos, pero entre los puntos 3 y 4 se debe modificar el valor de la clave de Google APIs (ver capítulo 5.7.3 CERTILOC MAPS y las referencias [19] y [20]).

Los módulos CERTILOC, TSA, DSS y TESTER no necesitan instalación, puesto que son archivos ejecutables. No obstante, en caso de duda, se puede mirar los Anexos de [1] para más información.

Requisitos previos de hardware y software

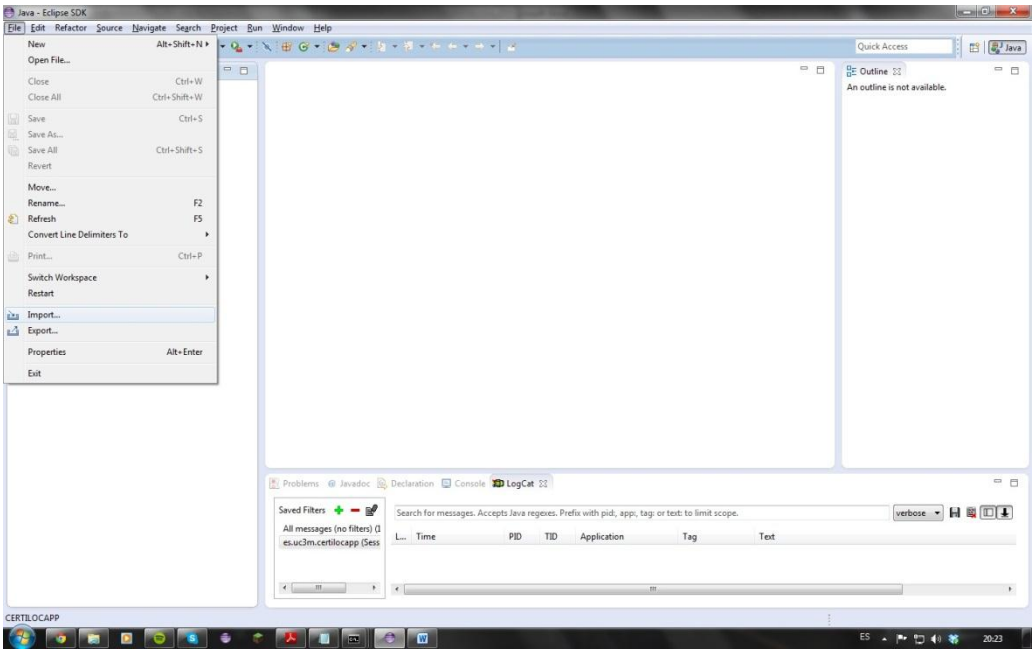
A nivel hardware, es necesario disponer de un ordenador de sobremesa y un dispositivo móvil con al menos 100Mb de espacio libre en una tarjeta de memoria externa. Se necesita tener el dispositivo móvil conectado al ordenador mediante cable USB.

A nivel software, se debe tener lo siguiente en cada dispositivo:

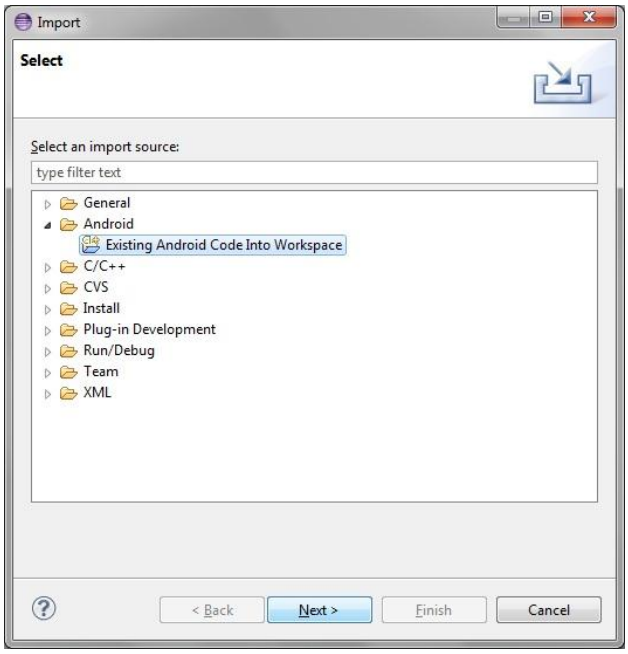
- Ordenador: Eclipse, Android SDK y los driver del dispositivo móvil.
- Dispositivo móvil: sistema operativo Android versión 3.0 o superior.

Procedimiento de Instalación

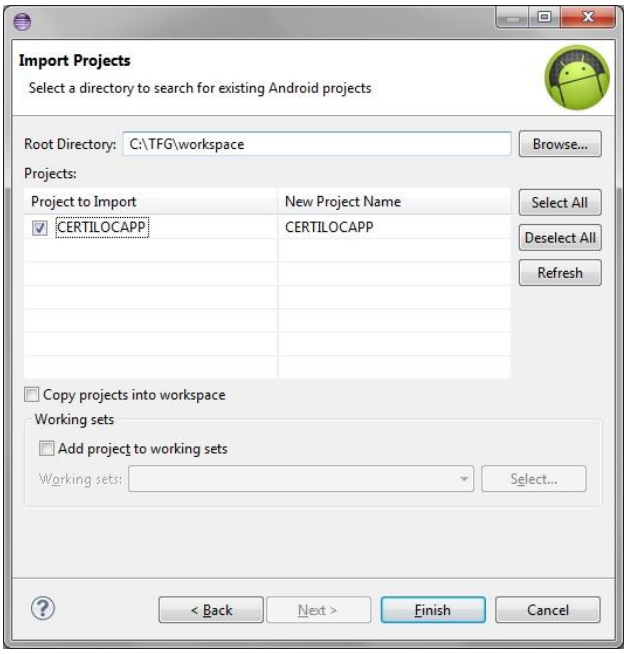
1. Lanzar el entorno de desarrollo Eclipse e ir al menú *File – Import…*



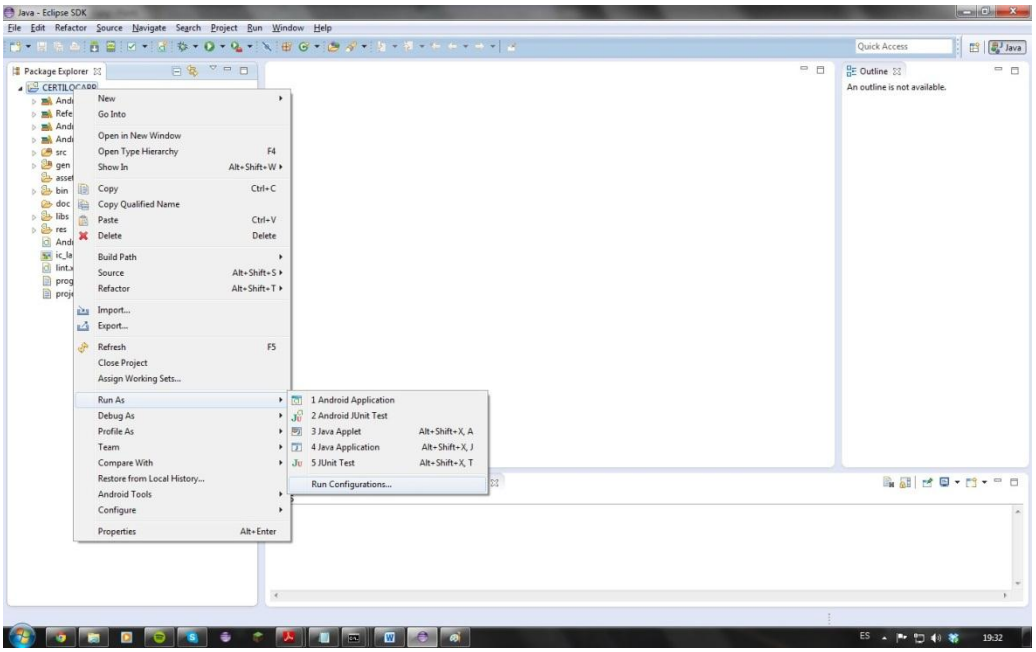
2. Seleccionar la opción *Android – Existing Code Into Workspace* y pulsar en *Next*.



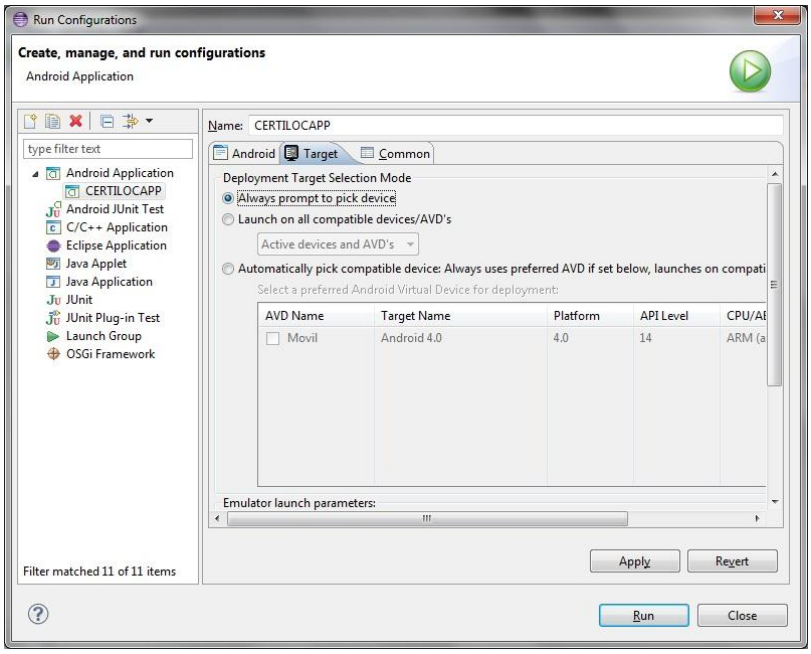
3. Pulsar el botón *Browse…* y seleccionar el directorio donde se encuentre almacenado el código de la aplicación. Después marcar el proyecto CERTILOC APP y pulsar en *Finish.*



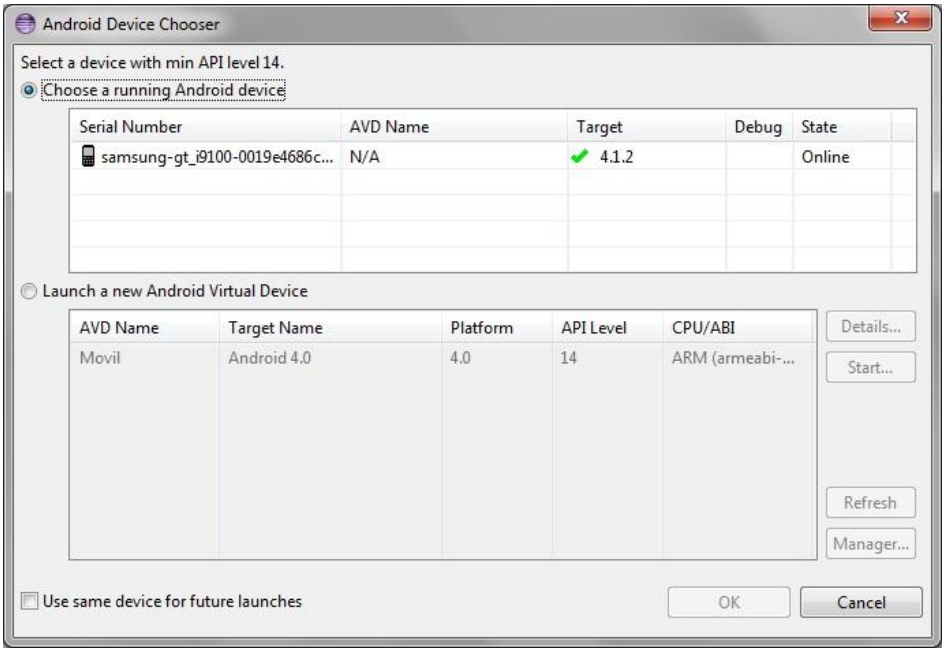
4. Pulsar con el botón derecho del ratón (menú contextual) en el proyecto y seleccionar *Run As – Run Configurations…*



5. Entrar en la pestaña *Target* y marcar *Always prompt to pick device*. De este modo, siempre que se ejecute solicitará seleccionar dónde ejecutar la aplicación. Pulsar en Run para comenzar al ejecución



6. Marcar *Choose a running Android device* y seleccionar en el dipositivo móvil que aparezca. Si no apareciera ninguno, comprobar que esté conectado el dispotivo móvil al ordenador mediante cable USB y que los drivers están instalados correctamente. Pulsar en OK.



7. La aplicación se instalará en el dispositivo y comenzará su ejecución